

Construction of Full-Diversity LDPC Lattices for Block-Fading Channels

Hassan Khodaiemehr, Mohammad-Reza Sadeghi and Daniel Panario, *Senior Member, IEEE*

Abstract

LDPC lattices were the first family of lattices which have an efficient decoding algorithm in high dimensions over an AWGN channel. Considering Construction D' of lattices with one binary LDPC code as underlying code gives the well known Construction A LDPC lattices or 1-level LDPC lattices. Block-fading channel (BF) is a useful model for various wireless communication channels in both indoor and outdoor environments. Frequency-hopping schemes and orthogonal frequency division multiplexing (OFDM) can conveniently be modelled as block-fading channels. Applying lattices in this type of channel entails dividing a lattice point into multiple blocks such that fading is constant within a block but changes, independently, across blocks. The design of lattices for BF channels offers a challenging problem, which differs greatly from its counterparts like AWGN channels. Recently, the original binary Construction A for lattices, due to Forney, have been generalized to a lattice construction from totally real and complex multiplication fields. This generalized Construction A of lattices provides signal space diversity intrinsically, which is the main requirement for the signal sets designed for fading channels. In this paper we construct full diversity LDPC lattices for block-fading channels using Construction A over totally real number fields. We propose a new iterative decoding method for these family of lattices which has complexity that grows linearly in the dimension of the lattice. In order to implement our decoding algorithm, we propose the definition of a parity check matrix and Tanner graph for full diversity Construction A lattices. We also prove that the constructed LDPC lattices together with the proposed decoding method admit diversity order $n - 1$ over an n -block-fading channel.

Index Terms

Hassan Khodaiemehr and Mohammad-Reza Sadeghi are with the Department of Mathematics and Computer Science, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran. Emails: {h.khodaiemehr, msadeghi}@aut.ac.ir.

Daniel Panario, is with the School of Mathematics and Statistics, Carleton University, Ottawa, Canada. Email: daniel@math.carleton.ca.

Part of this work has been presented in [1] at ISIT 2016, Spain.

LDPC lattice, full diversity, algebraic number fields.

I. INTRODUCTION

A lattice in \mathbb{R}^N is a subgroup of \mathbb{R}^N which is isomorphic to \mathbb{Z}^N and spans the real vector space \mathbb{R}^N [2]. Lattices have been extensively addressed for the problem of coding in Additive White Gaussian Noise (AWGN) channels. Communication on an AWGN channel using lattices is a communication without power constraints that has been investigated by Poltyrev [3]. In such a communication system, instead of coding rate and capacity, normalized logarithmic density (NLD) and generalized capacity C_∞ are used, respectively.

There exist different methods to construct lattices. One of the most distinguished ones is constructing lattices based on codes, where Construction A, D and D' have been proposed (for details see e.g. [2]). In [4], it is shown that the sphere bound can be approached by a large class of coset codes or multilevel coset codes with multistage decoding, including Construction D lattices and other certain binary lattices. Their results are based on channel coding theorems of information theory. As a result of their study, the concept of volume-to-noise (VNR) ratio was introduced as a parameter for measuring the efficiency of lattices [4]. The subsequent challenge in lattice theory has been to find structured classes of lattices that can be encoded and decoded with reasonable complexity in practice, and with performance that can approach the sphere-bound. This results in the transmission with arbitrary small error probability whenever VNR approaches to 1. A capacity-achieving lattice can raise to a capacity-achieving lattice code by selecting a proper shaping region [5], [6].

Applying maximum-likelihood (ML) decoding for lattices in high dimensions is infeasible and forced researchers to apply other low complexity decoding methods for lattices to obtain practical capacity-achieving lattices. Integer lattices built by Construction A, D and D' can be decoded with linear complexity based on soft-decision decoding of their underlying linear binary and non-binary codes [7], [8], [9], [10], [11], [12], [13], [14]. The search for sphere-bound-achieving and capacity-achieving lattices and lattice codes followed by proposing low density parity-check (LDPC) lattices [8], low density lattice codes (LDLC) [15] and integer low-density lattices based on Construction A (LDA) [9]. Turbo lattices, based on Construction D [12], and polar lattices [16] are other families of lattices with practical decoding methods.

Among the above family of lattices, LDPC lattices are those that have sparse parity check matrices, obtained by using a set of nested binary LDPC codes as underlying codes, together with

Construction D'. If the number of underlying LDPC codes (or the level of construction) is one, Construction D' coincides with Construction A and 1-level LDPC lattices are obtained [17]. The theory behind Construction A is well understood. There is a series of dualities between theoretical properties of the underlying codes and their resulting lattices. For example there are connections between the dual of the code and the dual of the lattice, or between the weight enumerator of the code and the theta series of the lattice [2], [18]. Construction A has been generalized in different directions; for example a generalized construction from the cyclotomic field $\mathbb{Q}(\xi_p)$, $\xi_p = e^{2\pi i/p}$ and p a prime, is presented in [18]. Then in [19], a generalized construction of lattices over a number field from linear codes is proposed. There is consequently a rich literature studying Construction A over different alphabets and for different tasks.

Lattices have been also considered for transmission over fading channels. Specifically, algebraic lattices, defined as lattices obtained via the ring of integers of a number field, provide efficient modulation schemes [20] for fast Rayleigh fading channels. Families of algebraic lattices are known to reach full diversity, the first design criterion for fading channels; see the definition of full diversity in Section V-B. Algebraic lattice codes are then natural candidates for the design of codes for block-fading channels.

The block-fading channel (BF) [21] is a useful channel model for a class of slowly-varying wireless communication channels. Frequency-hopping schemes and orthogonal frequency division multiplexing (OFDM), applied in many wireless communication systems standards, can conveniently be modelled as block-fading channels. In a BF channel a codeword spans a finite number n of independent fading blocks. As the channel realizations are constant within blocks, no codeword is able to experience all the states of the channel; this implies that the channel is non-ergodic and therefore it is not information stable. It follows that the Shannon capacity of this channel is zero [22]. As far as we are aware, all available lattice based schemes on block-fading channels were proposed by using optimal decoders [23] which have exponential complexity in the worst-case. In this paper we propose full diversity LDPC lattices and their decoding method which is a mix of optimal decoding in small dimensions and iterative decoding. The proposed decoding algorithm makes it tractable to decode high-dimension LDPC lattices on the BF channel.

The rest of this paper is organized as follows. In Section II, we provide preliminaries about lattices and algebraic number theory. In Section III, we present the available methods for constructing full diversity lattices from totally real number fields. The introduction of the full-

diversity 1-level LDPC lattices is also given in this section. In Section IV, the introduction of monogenic number fields, as the tools for constructing full-diversity 1-level LDPC lattices, is provided. In Section V, the system model is described for the Rayleigh block-fading channel. The available methods for evaluating the performance of finite and infinite lattice constellations over fading and block-fading channels are also discussed in this section. In Section VI, our construction of full diversity lattices is given. In Section VII, a new decoding method is proposed for full diversity 1-level LDPC lattices in high dimensions. The analysis of the proposed decoding method is also given in this section. In Section VIII, we give computer simulations, providing decoding performance and a comparison against available bounds. Section IX contains concluding remarks.

Notation: Matrices and vectors are denoted by bold upper and lower case letters. The i th element of vector \mathbf{a} is denoted by a_i and the entry (i, j) of a matrix \mathbf{A} is denoted by $A_{i,j}$; $[\]^t$ denotes the transposition for vectors and matrices.

II. PRELIMINARIES ON LATTICES AND ALGEBRAIC NUMBER THEORY

In order to make this work self-contained, general notations and basic definitions of algebraic number theory and lattices are given next. We reveal the connection between lattices and algebraic number theory at the end of this section.

A. Algebraic number theory

Let K and L be two fields. If $K \subset L$, then L is a field extension of K denoted by L/K . The dimension of L as vector space over K is the degree of L over K , denoted by $[L : K]$. Any finite extension of \mathbb{Q} is a number field.

Let L/K be a field extension, and let $\alpha \in L$. If there exists a non-zero irreducible monic polynomial $p_\alpha \in K[x]$ such that $p_\alpha(\alpha) = 0$, α is algebraic over K . Such a polynomial is the minimal polynomial of α over K . If all the elements of L are algebraic over K , L is an algebraic extension of K .

Definition 1: Let K be an algebraic number field of degree n ; $\alpha \in K$ is an algebraic integer if it is a root of a monic polynomial with coefficients in \mathbb{Z} . The set of algebraic integers of K is the ring of integers of K , denoted by O_K . The ring O_K is also called the maximal order of K .

If K is a number field, then $K = \mathbb{Q}(\theta)$ for an algebraic integer $\theta \in O_K$ [24]. For a number field K of degree n , the ring of integers O_K forms a free \mathbb{Z} -module of rank n .

Definition 2: Let $\{\omega_1, \dots, \omega_n\}$ be a basis of the \mathbb{Z} -module O_K , so that we can uniquely write any element of O_K as $\sum_{i=1}^n a_i \omega_i$ with $a_i \in \mathbb{Z}$ for all i . Then, $\{\omega_1, \dots, \omega_n\}$ is an integral basis of K .

Theorem 1: [24, p. 41] Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over \mathbb{Q} . There are exactly n embeddings $\sigma_1, \dots, \sigma_n$ of K into \mathbb{C} defined by $\sigma_i(\theta) = \theta_i$, for $i = 1, \dots, n$, where the θ_i 's are the distinct zeros in \mathbb{C} of the minimal polynomial of θ over \mathbb{Q} .

Definition 3: Let K be a number field of degree n and $x \in K$. The elements $\sigma_1(x), \dots, \sigma_n(x)$ are the conjugates of x and

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^n \sigma_i(x), \quad \text{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=1}^n \sigma_i(x), \quad (1)$$

are the norm and the trace of x , respectively.

For any $x \in K$, we have $N_{K/\mathbb{Q}}(x), \text{Tr}_{K/\mathbb{Q}}(x) \in \mathbb{Q}$. If $x \in O_K$, we have $N_{K/\mathbb{Q}}(x), \text{Tr}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$.

Definition 4: Let $\{\omega_1, \dots, \omega_n\}$ be an integral basis of K . The discriminant of K is defined as

$$d_K = \det(A)^2, \quad (2)$$

where A is the matrix $A_{i,j} = \sigma_j(\omega_i)$, for $i, j = 1, \dots, n$. The discriminant of a number field belongs to \mathbb{Z} and it is independent of the choice of a basis.

Definition 5: Let $\{\sigma_1, \dots, \sigma_n\}$ be the n embeddings of K into \mathbb{C} . Let r_1 be the number of embeddings with image in \mathbb{R} , the field of real numbers, and $2r_2$ the number of embeddings with image in \mathbb{C} so that $r_1 + 2r_2 = n$. The pair (r_1, r_2) is the signature of K . If $r_2 = 0$ we have a totally real algebraic number field. If $r_1 = 0$ we have a totally complex algebraic number field.

Definition 6: Let us order the σ_i 's so that, for all $x \in K$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, and $\sigma_{j+r_2}(x)$ is the complex conjugate of $\sigma_j(x)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. The canonical embedding $\sigma : K \rightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is the homomorphism defined by

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \dots, \sigma_{r_1+r_2}(x)). \quad (3)$$

If we identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with \mathbb{R}^n , the canonical embedding can be rewritten as $\sigma : K \rightarrow \mathbb{R}^n$

$$\begin{aligned} \sigma(x) = & (\sigma_1(x), \dots, \sigma_{r_1}(x), \Re \sigma_{r_1+1}(x), \Im \sigma_{r_1+1}(x), \\ & \dots, \Re \sigma_{r_1+r_2}(x), \Im \sigma_{r_1+r_2}(x)), \end{aligned} \quad (4)$$

where \Re denotes the real part and \Im the imaginary part.

Definition 7: A ring A is integrally closed in a field L if every element of L which is integral over A in fact lies in A . It is integrally closed if it is integrally closed in its quotient field.

Theorem 2: [25, p. 18] Let D be a Noetherian ring, that is, it satisfies the ascending chain condition on ideals, integrally closed, and such that every non-zero prime ideal is maximal. Then every ideal of D can be uniquely factored into prime ideals.

A ring satisfying the properties of Theorem 2 is a Dedekind ring. The ring of algebraic integers in a number field is a Dedekind ring.

Definition 8: Let A be a ring and x an element of some field L containing A . Then, x is integral over A if either one of the following conditions is satisfied:

- there exists a finitely generated non-zero A -module $M \subset L$ such that $xM \subset M$;
- the element x satisfies an equation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0,$$

with coefficients $a_i \in A$, and an integer $n \geq 1$. Such an equation is an integral equation.

Let A be a Dedekind ring, K its quotient field, L a finite separable extension of K , and B the integral closure of A in L . If \mathfrak{p} is a prime ideal of A , then $\mathfrak{p}B$ is an ideal of B and has a factorization

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \quad (5)$$

into primes of B , where $e_i \geq 1$. It is clear that a prime \mathfrak{P} of B occurs in this factorization if and only if \mathfrak{P} lies above \mathfrak{p} . Each e_i is called the ramification index of \mathfrak{P}_i over \mathfrak{p} , and is also written $e(\mathfrak{P}_i/\mathfrak{p})$. If \mathfrak{P} lies above \mathfrak{p} in B , we denote by $f(\mathfrak{P}/\mathfrak{p})$ the degree of the residue class field extension B/\mathfrak{P} over A/\mathfrak{p} , and call it the residue class degree or inertia degree.

Theorem 3: [25, p. 24] Let A be a Dedekind ring, K its quotient field, L a finite separable extension of K , and B the integral closure of A in L . Let \mathfrak{p} be a prime of A . Then

$$[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}). \quad (6)$$

When L/K is a Galois extension of degree n , this simplifies to $n = efg$, where g is the number of primes \mathfrak{P} of B above \mathfrak{p} . In other words, $e(\mathfrak{P}/\mathfrak{p}) = e$ and $f(\mathfrak{P}/\mathfrak{p}) = f$ for all $\mathfrak{P}|\mathfrak{p}$. If $e_{\mathfrak{P}} = f_{\mathfrak{P}}$ for all $\mathfrak{P}|\mathfrak{p}$, then \mathfrak{p} *splits completely* in L . In that case, there are exactly $[L : K]$ primes of B lying above \mathfrak{p} . A prime \mathfrak{p} in K is *ramified* in a number field L if the prime ideal factorization (5) has some e_i greater than 1. If every e_i equals 1, \mathfrak{p} is *unramified* in L . If $[L : K] = e(\mathfrak{P}/\mathfrak{p})$,

\mathfrak{P} is *totally ramified* above \mathfrak{p} . In this case, the residue class degree is equal to 1. Since \mathfrak{P} is the only prime of B lying above \mathfrak{p} , L is *totally ramified* over K . If the characteristic p of the residue class field A/\mathfrak{p} does not divide $e(\mathfrak{P}/\mathfrak{p})$, then \mathfrak{P} is *tamely ramified* over \mathfrak{p} (or L is tamely ramified over K). If it does, then \mathfrak{P} is *strongly ramified*.

B. Lattices

Any discrete additive subgroup Λ of the m -dimensional real space \mathbb{R}^m is a lattice. Every lattice Λ has a basis $\mathcal{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\} \subseteq \mathbb{R}^m$, $n \leq m$, where every $\mathbf{x} \in \Lambda$ can be represented as an integer linear combination of vectors in \mathcal{B} . The $n \times m$ matrix \mathbf{M} with $\mathbf{b}_1, \dots, \mathbf{b}_n$ as rows, is a generator matrix for the lattice. The rank of the lattice is n and its dimension is m . If $n = m$, the lattice is a full-rank lattice. In this paper, we consider only full-rank lattices. A lattice Λ can be described in terms of a generator matrix \mathbf{M} by

$$\Lambda = \{\mathbf{x} = \mathbf{uM} \mid \mathbf{u} \in \mathbb{Z}^n\}. \quad (7)$$

When using lattices for coding, their Voronoi cells and volume always play an important role. For any lattice point \mathbf{p} of a lattice $\Lambda \subset \mathbb{R}^m$, its Voronoi cell is defined by

$$\mathcal{V}_\Lambda(\mathbf{p}) = \{\mathbf{x} \in \mathbb{R}^m, d(\mathbf{x}, \mathbf{p}) \leq d(\mathbf{x}, \mathbf{q}) \text{ for all } \mathbf{q} \in \Lambda\}. \quad (8)$$

All Voronoi cells are the same, thus $\mathcal{V}_\Lambda(\mathbf{p}) = \mathcal{V}_\Lambda(\mathbf{0}) \triangleq \mathcal{V}(\Lambda)$. The matrix $\mathbf{G} = \mathbf{MM}^t$ is a Gram matrix for the lattice. The determinant of the lattice $\det(\Lambda)$ is defined as the determinant of the matrix \mathbf{G} and the volume of the lattice is

$$\text{vol}(\Lambda) = \text{vol}(\mathcal{V}(\Lambda)) = \sqrt{\det(\mathbf{G})}. \quad (9)$$

Definition 9: A lattice Λ in \mathbb{R}^m is an integral lattice if its Gram matrix has coefficients in \mathbb{Z} . Indeed, a lattice Λ is integral if and only if $\langle x, y \rangle \in \mathbb{Z}$, for all $x, y \in \Lambda$, where \langle, \rangle is the regular inner product of \mathbb{R}^m .

The set of all vectors in \mathbb{R}^m whose inner product with all vectors of Λ is in \mathbb{Z} is another lattice, the dual lattice of Λ , denoted by Λ^* . The *normalized volume* of an n -dimensional lattice Λ is defined as $\det(\Lambda)^{2/n}$ [4]. This volume may be regarded as the volume of Λ per two dimensions.

Suppose that the points of a lattice Λ are sent over an unconstrained Additive White Gaussian Noise (AWGN) [3] channel, with noise variance σ^2 . Let the vector $\mathbf{x} \in \Lambda$ be transmitted over the unconstrained AWGN channel, then the received vector \mathbf{r} can be written as $\mathbf{r} = \mathbf{x} + \mathbf{e}$,

where $\mathbf{e} = (e_1, \dots, e_n)$ is the error term and its components are independently and identically distributed (i.i.d.) with $\mathcal{N}(0, \sigma^2)$. The *volume-to-noise ratio* (VNR) of the lattice Λ is defined as

$$\text{VNR} = \frac{\text{vol}(\Lambda)^{\frac{2}{n}}}{2\pi e \sigma^2}. \quad (10)$$

For large n , VNR is the ratio of the normalized volume of Λ to the normalized volume of a noise sphere of squared radius $n\sigma^2$ which is defined as generalized signal-to-noise ratio (SNR) in [8] and α^2 in [4]. Due to the geometric uniformity of lattices, the probability of error under maximum likelihood decoding of Λ is the probability that a white Gaussian n -tuple \mathbf{r} with noise variance σ^2 falls outside the Voronoi cell $\mathcal{V}(\mathbf{0}) = \mathcal{V}$.

Now we present definitions in algebraic lattice theory equivalent to the above definitions.

Definition 10: An integral lattice Γ is a free \mathbb{Z} -module of finite rank together with a positive definite symmetric bilinear form $\langle, \rangle : \Gamma \times \Gamma \rightarrow \mathbb{Z}$.

Definition 11: The discriminant of a lattice Γ , denoted $\text{disc}(\Gamma)$, is the determinant of $\mathbf{M}\mathbf{M}^t$ where \mathbf{M} is a generator matrix for Γ . The volume $\text{vol}(\mathbb{R}^n/\Gamma)$ of a lattice Γ is defined as $|\det(\mathbf{M})|$.

The discriminant is related to the volume of a lattice by

$$\text{vol}(\mathbb{R}^n/\Gamma) = \sqrt{\text{disc}(\Gamma)}. \quad (11)$$

Moreover, when Γ is integral, we have $\text{disc}(\Gamma) = |\Gamma^*/\Gamma|$, where Γ^* is the dual of the lattice Γ defined by

$$\Gamma^* = \{y \in \mathbb{R}^m \mid y \cdot x \in \mathbb{Z} \text{ for all } x \in \Gamma\}. \quad (12)$$

When $\Gamma = \Gamma^*$, the lattice Γ is unimodular.

The canonical embedding (4) gives a geometrical representation of a number field and makes the connection between algebraic number fields and lattices.

Theorem 4: [24, p. 155] Let $\{\omega_1, \omega_2, \dots, \omega_n\}$ be an integral basis of a number field K . The n vectors $\mathbf{v}_i = \sigma(\omega_i) \in \mathbb{R}^n$, $i = 1, \dots, n$ are linearly independent, so they define a full rank lattice $\Lambda = \Lambda(O_K) = \sigma(O_K)$.

Theorem 5: [26] Let d_K be the discriminant of a number field K . The volume of the fundamental parallelotope of $\Lambda(O_K)$ is given by

$$\text{vol}(\Lambda(O_K)) = 2^{-r_2} \sqrt{|d_K|}. \quad (13)$$

III. LATTICE CONSTRUCTIONS USING CODES

There exist many ways to construct lattices based on codes [2]. Here we mention a lattice construction from totally real and complex multiplication fields [19], which naturally generalizes Construction A of lattices from p -ary codes obtained from the cyclotomic field $\mathbb{Q}(\xi_p)$, with $\xi_p = e^{2\pi i/p}$ and p a prime number [18]. This contains the so-called Construction A of lattices from binary codes as a particular case.

A. Construction A of lattices

Given a number field K and a prime \mathfrak{p} of \mathcal{O}_K above p where $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f}$, let \mathcal{C} be an (N, k) linear code over \mathbb{F}_{p^f} . The Construction A of lattices using underlying code \mathcal{C} and number field K is given in [19].

Definition 12: Let $\rho : \mathcal{O}_K^N \rightarrow \mathbb{F}_{p^f}^N$ be the mapping defined by the reduction modulo the ideal \mathfrak{p} in each of the N coordinates. Define $\Gamma_{\mathcal{C}}$ to be the preimage of \mathcal{C} in \mathcal{O}_K^N , i.e.,

$$\Gamma_{\mathcal{C}} = \{\mathbf{x} \in \mathcal{O}_K^N \mid \rho(\mathbf{x}) = \mathbf{c}, \mathbf{c} \in \mathcal{C}\}. \quad (14)$$

We conclude that $\Gamma_{\mathcal{C}}$ is a \mathbb{Z} -module of rank nN . When K is totally real, $\rho^{-1}(\mathcal{C})$ forms a lattice with the following symmetric bilinear form [19]

$$\langle x, y \rangle = \sum_{i=1}^N \text{Tr}_{K/\mathbb{Q}}(\alpha x_i y_i), \quad (15)$$

where $\mathbf{x} = (x_1, \dots, x_N)$ and $\mathbf{y} = (y_1, \dots, y_N)$ are vectors in \mathcal{O}_K^N , $\alpha \in \mathcal{O}_K$ is a totally positive element, meaning that $\sigma_i(\alpha) > 0$ for all i , and $\text{Tr}_{K/\mathbb{Q}}$ is defined in (1). Thus, $\Gamma_{\mathcal{C}}$ together with the bilinear form (15) is an integral lattice. A similar construction is obtained from a CM-field [19]. A CM-field is a totally imaginary quadratic extension of a totally real number field. If K is a CM-field and $\alpha \in \mathcal{O}_K \cap \mathbb{R}$ is totally positive, then $\rho^{-1}(\mathcal{C})$ forms a lattice with the following symmetric bilinear form

$$\langle x, y \rangle = \sum_{i=1}^N \text{Tr}_{K/\mathbb{Q}}(\alpha x_i \bar{y}_i), \quad (16)$$

where \bar{y}_i denotes the complex conjugate of y_i . If K is totally real, then $\bar{y}_i = y_i$, and this notation treats both cases of totally real and CM-fields at the same time. It has been shown that if $\mathcal{C} \subset \mathcal{C}^\perp$, then $\sum_{i=1}^N \text{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i) \in p\mathbb{Z}$, and thus the symmetric bilinear form can be normalized by a factor $1/p$, or equivalently, by choosing $\alpha = 1/p$ [19].

Other variations of the above construction have been considered in the literature. The case $N = 1$ is considered in [27] where the problem reduces to understanding which lattices can

be obtained on the ring of integers of a number field. The case that K is the cyclotomic field $\mathbb{Q}(\xi_p)$ has been considered in [18]. In [28], the prime ideal \mathfrak{p} is considered to be $(2m)$, yielding codes over a ring of polynomials with coefficients modulo $2m$. In [29], \mathfrak{p} is considered to be $(2 - \xi_p + \xi_p^{-1})$ and the resulting codes are over \mathbb{F}_p . Quadratic extensions $K = \mathbb{Q}(\sqrt{-l})$ are considered in [30] and [31] where the reduction is done by the ideal (p^e) and the resulting codes are over the ring $O_K/p^e O_K$.

A generator matrix for the lattice $\Gamma_{\mathcal{C}}$ is computed in [19]. Let K be a Galois extension and the prime \mathfrak{p} be chosen so that \mathfrak{p} is totally ramified. Therefore, we have $pO_K = \mathfrak{p}^n$. Now, let $\mathcal{C} \subset \mathbb{F}_p^N$ be a linear code over \mathbb{F}_p of length N . Since $\Gamma_{\mathcal{C}}$ has rank nN as a free \mathbb{Z} -module, we obtain the \mathbb{Z} -basis of $\Gamma_{\mathcal{C}}$. Let $\{\omega_1, \dots, \omega_n\}$ be a \mathbb{Z} -basis of O_K . Then, a generator matrix for the lattice formed by O_K together with the standard trace form $\langle w, z \rangle = \text{Tr}_{K/\mathbb{Q}}(wz)$, $w, z \in O_K$, is given by

$$\mathbf{M} = [\sigma_j(\omega_i)]_{i,j=1}^n. \quad (17)$$

The prime ideal \mathfrak{p} is a \mathbb{Z} -module of rank n . It then has a \mathbb{Z} -basis $\{\mu_1, \dots, \mu_n\}$ where $\mu_i = \sum_{j=1}^n \mu_{i,j} \omega_j$. Thus

$$[\sigma_j(\mu_i)]_{i,j=1}^n = \mathbf{D}\mathbf{M}, \quad (18)$$

where $\mathbf{D} = [\mu_{i,j}]_{i,j=1}^n$.

Theorem 6: [19, Proposition 1] The lattice $\Gamma_{\mathcal{C}}$ is a sublattice of O_K^N with discriminant

$$\text{disc}(\Gamma_{\mathcal{C}}) = d_K^N (p^f)^{2(N-k)}, \quad (19)$$

where $d_K = (\det([\sigma_i(\omega_j)]_{i,j=1}^n))^2$ is the discriminant of K . The lattice $\Gamma_{\mathcal{C}}$ is given by the generator matrix

$$\mathbf{M}_{\mathcal{C}} = \begin{bmatrix} \mathbf{I}_k \otimes \mathbf{M} & \mathbf{A} \otimes \mathbf{M} \\ \mathbf{0}_{n(N-k) \times nk} & \mathbf{I}_{N-k} \otimes \mathbf{D}\mathbf{M} \end{bmatrix}, \quad (20)$$

where \otimes is the tensor product of matrices, $\begin{bmatrix} \mathbf{I}_k & \mathbf{A} \end{bmatrix}$ is a generator matrix of \mathcal{C} , \mathbf{M} is the matrix of embeddings of a \mathbb{Z} -basis of O_K given in (17), and $\mathbf{D}\mathbf{M}$ is the matrix of embeddings of a \mathbb{Z} -basis of \mathfrak{p} in (18).

B. LDPC lattices from Construction A and Construction D'

Assume that \mathcal{C} is a linear code over \mathbb{F}_p where p is a prime number, i.e. $\mathcal{C} \subseteq \mathbb{F}_p^N$. Let d_{\min} denote the minimum distance of \mathcal{C} . A lattice Λ constructed based on Construction A [2] can be derived from \mathcal{C} by:

$$\Lambda = p\mathbb{Z}^N + \epsilon(\mathcal{C}), \quad (21)$$

where $\epsilon: \mathbb{F}_p^N \rightarrow \mathbb{R}^N$ is the embedding function which sends a vector in \mathbb{F}_p^N to its real version. In this work, we are particularly interested in binary codes and lattices with $p = 2$.

Construction D' converts a set of parity checks defined by a family of nested codes into congruences for a lattice [2]. This construction is a good tool to produce lattices based on LDPC codes. Let $\mathcal{C}_0 \supseteq \mathcal{C}_1 \supseteq \dots \supseteq \mathcal{C}_a$ be a family of nested linear codes, where \mathcal{C}_ℓ has parameter $[n, k_\ell, d_{\min}^\ell]$, for $0 \leq \ell \leq a$. Let $\{\mathbf{h}_1, \dots, \mathbf{h}_N\}$ be a linearly independent set of vectors in \mathbb{F}_2^N and the code \mathcal{C}_ℓ be defined by the $r_\ell = N - k_\ell$ parity check vectors $\mathbf{h}_1, \dots, \mathbf{h}_{r_\ell}$. Define the new lattice Λ consisting of those $\mathbf{x} \in \mathbb{Z}^N$ that satisfy the congruences $\mathbf{h}_j \cdot \mathbf{x} \equiv 0 \pmod{2^{\ell+1}}$ for $0 \leq \ell \leq a$ and $r_{a-\ell-1} + 1 \leq j \leq r_{a-\ell}$. The number $a + 1$ is the level of the construction.

By multiplying the modular equations by appropriate powers of 2, we can restate Construction D' [8]. Indeed, $\mathbf{x} \in \Lambda$ if and only if $\mathbf{H}_\Lambda \mathbf{x}^t = \mathbf{0} \pmod{2^{a+1}}$ where

$$\mathbf{H}_\Lambda = [\mathbf{h}_1, \dots, \mathbf{h}_{r_0}, \dots, 2^a \mathbf{h}_{r_{a-1}+1}, \dots, 2^a \mathbf{h}_{r_a}]^t. \quad (22)$$

Then, \mathbf{H}_Λ constitutes the parity check matrix of Λ . When the underlying codes are binary LDPC codes, the lattice Λ constructed based on Construction D' and associated to this \mathbf{H}_Λ is an $(a+1)$ -level LDPC lattice. The Tanner graph of these lattices can be constructed based on their parity check matrices \mathbf{H}_Λ and used for decoding purposes [8].

Definition 13: A 1-level LDPC lattice Λ is a lattice based on Construction D' along with a binary linear LDPC code \mathcal{C} as its underlying code. Equivalently, $\mathbf{x} \in \mathbb{Z}^N$ is in Λ if $\mathbf{H}_\mathcal{C} \mathbf{x}^t = \mathbf{0} \pmod{2}$, where $\mathbf{H}_\mathcal{C}$ is the parity-check matrix of \mathcal{C} [13], [17], [32].

Proposition 1: A 1-level LDPC lattice Λ is equal to a lattice Λ_1 constructed following Construction A using the same underlying code \mathcal{C} [17].

The generator matrix of 1-level LDPC lattice Λ using the underlying code \mathcal{C} is of the form [2], [13]:

$$\mathbf{G}_\Lambda = \begin{bmatrix} \mathbf{I}_k & \mathbf{P}_{k \times (N-k)} \\ \mathbf{0}_{(N-k) \times k} & 2\mathbf{I}_{N-k} \end{bmatrix}, \quad (23)$$

where $\mathbf{G}_C = \begin{bmatrix} \mathbf{I}_k & \mathbf{P}_{k \times (N-k)} \end{bmatrix}$ is the generator matrix of \mathcal{C} in systematic form, k is the rank of \mathcal{C} and N is the code length of \mathcal{C} . The matrices \mathbf{I}_k and $\mathbf{0}_{(N-k) \times k}$ are the identity matrix of size k and the all zero matrix of size $(N-k) \times k$, respectively.

Example 1: This example is discussed in [19]. Let p be an odd prime, and let ξ_p be a primitive p th root of unity. Consider the cyclotomic field $K = \mathbb{Q}(\xi_p)$ with the ring of integers $O_K = \mathbb{Z}[\xi_p]$. The degree of K over \mathbb{Q} is $p-1$, and p is totally ramified, with $pO_K = (1 - \xi_p)^{p-1}$. Thus, taking the prime ideal $\mathfrak{p} = (1 - \xi_p)$ with the residue field $O_K/\mathfrak{p} \simeq \mathbb{F}_p$, the bilinear form $\langle x, y \rangle = \sum_{i=1}^N \text{Tr}_{K/Q}(x_i y_i)$ and a linear code \mathcal{C} over \mathbb{F}_p , then Γ_C yields the so-called Construction A as described above. Since $\mathbb{Q}(\xi_p)$ is a CM-field, we can use the bilinear form corresponding to (16) with $\alpha = 1/p$. By using this bilinear form, the generator matrix is as follows

$$\mathbf{M}_C = \frac{1}{\sqrt{p}} \begin{bmatrix} \mathbf{I}_k & \mathbf{P}_{k \times (N-k)} \\ \mathbf{0}_{(N-k) \times k} & p\mathbf{I}_{N-k} \end{bmatrix}. \quad (24)$$

It has been proved in [19] that if $\mathcal{C} \subset \mathcal{C}^\perp$, then Γ_C is an integral lattice of rank $N(p-1)$. Our particular case is based on Construction A of lattices from codes when $p = 2$. In such case, $\xi_p = -1$, $O_K = \mathbb{Z}$, and $\mathfrak{p} = 2\mathbb{Z}$. \square

Next, we present the definition of 1-level LDPC lattices using algebraic number fields.

Definition 14: Let \mathcal{C} be a binary LDPC code of length N and dimension k . Consider the number field K with the ring of integers O_K . Let n be the degree of K over \mathbb{Q} and \mathfrak{p} be a prime in O_K with residue field $O_K/\mathfrak{p} \simeq \mathbb{F}_2$. Define $\rho : O_K^N \rightarrow \mathbb{F}_2^N$ as the componentwise reduction modulo \mathfrak{p} and $\sigma^i : O_K^i \rightarrow \mathbb{R}^{in}$, for positive integer i , as

$$\sigma^i(x_1, \dots, x_i) = (\sigma(x_1), \dots, \sigma(x_i)),$$

where σ is the canonical embedding in (4). Let $\{\omega_1, \dots, \omega_n\}$ be the integral basis for O_K . Define $\sigma^{-1} : \sigma(O_K) \rightarrow O_K$ such that for $x = \sum_{l=1}^n u_{l,i} \omega_l$ in O_K

$$\sigma^{-1}(\sigma_1(x), \dots, \sigma_n(x)) = x.$$

Define $(\sigma^i)^{-1}$ similarly to σ^i but replacing σ with σ^{-1} . Then, $\Lambda = \sigma^N(\Gamma_C) = \sigma^N(\rho^{-1}(\mathcal{C}))$ is the 1-level LDPC lattice based on the number field K . The parity check matrix \mathbf{H}_Λ for Λ is an $n(N-k) \times nN$ matrix over \mathbb{F}_2 of rank $n(N-k)$ such that

$$\Lambda = \{ \mathbf{x} \in \sigma^N(O_K) \mid \rho((\sigma^{N-k})^{-1}(\mathbf{xH}^t)) = \mathbf{0}_{1 \times (N-k)} \}. \quad (25)$$

Theorem 7: Let \mathcal{C} be a binary LDPC code of length N and dimension k . Let \mathbf{H} and $\mathbf{G} = \begin{bmatrix} \mathbf{I}_k & \mathbf{A} \end{bmatrix}$ be the parity check and generator matrices of \mathcal{C} , respectively. Consider the Galois

extension K/\mathbb{Q} with the ring of integers O_K . Let n be the degree of K over \mathbb{Q} and let 2 be totally ramified in O_K . The prime \mathfrak{p} is chosen above 2 so that $2O_K = \mathfrak{p}^n$ with residue field $O_K/\mathfrak{p} \simeq \mathbb{F}_2$. Then, $\mathbf{H}_\Lambda = \mathbf{H} \otimes \mathbf{I}_n$ is the parity check matrix of 1-level LDPC lattices $\Lambda = \sigma^N(\Gamma_{\mathcal{C}}) = \sigma^N(\rho^{-1}(\mathcal{C}))$.

Proof: Based on the assumed conditions and Theorem 6, the generator matrix of Λ has the following form

$$\mathbf{M}_\Lambda = \begin{bmatrix} \mathbf{I}_k \otimes \mathbf{M} & \mathbf{A} \otimes \mathbf{M} \\ \mathbf{0}_{n(N-k) \times nk} & \mathbf{I}_{N-k} \otimes \mathbf{D}\mathbf{M} \end{bmatrix}.$$

Let $\mathbf{u} = (u_1, \dots, u_{nN})$ be an integer vector. First we show that $\rho((\sigma^{N-k})^{-1}(\mathbf{u}\mathbf{M}_\Lambda\mathbf{H}_\Lambda^t)) = \mathbf{0}$. To this end,

$$\begin{aligned} \mathbf{M}_\Lambda\mathbf{H}_\Lambda^t &= \begin{bmatrix} [\mathbf{I}_k \ \mathbf{A}] \otimes \mathbf{M} \\ [\mathbf{0}_{(N-k) \times k} \ \mathbf{I}_{N-k}] \otimes \mathbf{D}\mathbf{M} \end{bmatrix} (\mathbf{H} \otimes \mathbf{I}_n)^t \\ &= \begin{bmatrix} [\mathbf{I}_k \ \mathbf{A}] \mathbf{H}^t \otimes \mathbf{M} \\ [\mathbf{0}_{(N-k) \times k} \ \mathbf{I}_{N-k}] \mathbf{H}^t \otimes \mathbf{D}\mathbf{M} \end{bmatrix}. \end{aligned}$$

The \mathbb{Z} -linearity of $(\sigma^{N-k})^{-1}$ implies the sufficiency of proving $\rho((\sigma^{N-k})^{-1}(\mathbf{b}_i)) = \mathbf{0}$, where \mathbf{b}_i is the i th row of $\mathbf{M}_\Lambda\mathbf{H}_\Lambda^t$, for $i = 1, \dots, nN$. Since \mathbf{H} and $[\mathbf{I}_k \ \mathbf{A}]$ are the parity check matrix and the generator matrix of the binary code \mathcal{C} , respectively, $[\mathbf{I}_k \ \mathbf{A}] \mathbf{H}^t = 2\mathbf{Z}$ for a $k \times (N-k)$ integer matrix \mathbf{Z} . On the other hand, $[\mathbf{0}_{(N-k) \times k} \ \mathbf{I}_{N-k}] \mathbf{H}^t = \mathbf{H}_{N-k}$, where \mathbf{H}_{N-k} is the last $N-k$ rows of \mathbf{H}^t . For $1 \leq i \leq kn$, let $r_i = \lfloor \frac{i}{n} \rfloor + 1$, where $\lfloor c \rfloor$ is the floor of a real number c , and $s_i = i - (r_i - 1)n$. Then

$$\mathbf{b}_i = (2z_{r_i,1}\mathbf{M}_{s_i}, 2z_{r_i,2}\mathbf{M}_{s_i}, \dots, 2z_{r_i,N-k}\mathbf{M}_{s_i}),$$

in which $\mathbf{Z}_{r_i} = (z_{r_i,1}, \dots, z_{r_i,N-k})$ and $\mathbf{M}_{s_i} = (\sigma_1(\omega_{s_i}), \dots, \sigma_n(\omega_{s_i}))$ are r_i th and s_i th rows of \mathbf{Z} and \mathbf{M} , respectively. Finally,

$$\begin{aligned} &\rho((\sigma^{N-k})^{-1}(\mathbf{b}_i)) \\ &= \rho((\sigma^{N-k})^{-1}(2z_{r_i,1}\mathbf{M}_{s_i}, \dots, 2z_{r_i,N-k}\mathbf{M}_{s_i})) \\ &= \rho(2z_{r_i,1}\sigma^{-1}(\mathbf{M}_{s_i}), \dots, 2z_{r_i,N-k}\sigma^{-1}(\mathbf{M}_{s_i})) \\ &= \rho(2z_{r_i,1}\omega_{s_i}, \dots, 2z_{r_i,N-k}\omega_{s_i}) \\ &= \mathbf{0}, \end{aligned}$$

where the last equation follows from the fact that

$$(2z_{r_i,1}\omega_{s_i}, \dots, 2z_{r_i,N-k}\omega_{s_i}) \in (2O_K)^{N-k} \subset \mathfrak{p}^{N-k}.$$

For $kn+1 \leq i \leq nN$, let $r_i = \lfloor \frac{i}{n} \rfloor - k + 1$, and $s_i = i - (r_i + k - 1)n$. Consider $\{\mu_1, \dots, \mu_n\}$ as the \mathbb{Z} -basis of \mathfrak{p} . Then

$$\mathbf{b}_i = (h_{r_i,1}\mathbf{P}_{s_i}, h_{r_i,2}\mathbf{P}_{s_i}, \dots, h_{r_i,N-k}\mathbf{P}_{s_i}),$$

where $(h_{r_i,1}, \dots, h_{r_i,N-k})$ and $\mathbf{P}_{s_i} = (\sigma_1(\mu_{s_i}), \dots, \sigma_n(\mu_{s_i}))$ are the r_i th and s_i th rows of \mathbf{H}_{N-k} and \mathbf{DM} , respectively. In this case

$$\begin{aligned} & \rho((\sigma^{N-k})^{-1}(\mathbf{b}_i)) \\ &= \rho((\sigma^{N-k})^{-1}(h_{r_i,1}\mathbf{P}_{s_i}, \dots, h_{r_i,N-k}\mathbf{P}_{s_i})) \\ &= \rho(h_{r_i,1}\sigma^{-1}(\mathbf{P}_{s_i}), \dots, h_{r_i,N-k}\sigma^{-1}(\mathbf{P}_{s_i})) \\ &= \rho(h_{r_i,1}\mu_{s_i}, \dots, h_{r_i,N-k}\mu_{s_i}) \\ &= \mathbf{0}. \end{aligned}$$

Now, let $\mathbf{x} \in \sigma^N(O_K)$ such that $\rho((\sigma^{N-k})^{-1}(\mathbf{x}\mathbf{H}_\Lambda^t)) = \mathbf{0}$. We show that $\mathbf{x} \in \Lambda$. For the sake of this, we have

$$\mathbf{x} = (\sigma_1(x_1), \dots, \sigma_n(x_1), \dots, \sigma_1(x_N), \dots, \sigma_n(x_N)),$$

where $\tilde{\mathbf{x}} = (x_1, \dots, x_N) \in O_K^N$. Then

$$\begin{aligned} \mathbf{x}\mathbf{H}_\Lambda^t &= \mathbf{x} [\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_{n(N-k)}]^t \\ &= (\mathbf{x} \cdot \mathbf{h}_1^t, \mathbf{x} \cdot \mathbf{h}_2^t, \dots, \mathbf{x} \cdot \mathbf{h}_{n(N-k)}^t), \end{aligned}$$

where $\mathbf{x} \cdot \mathbf{h}_i^t$ is the inner product of \mathbf{x} and the i th column of \mathbf{H}_Λ^t , \mathbf{h}_i , for $i = 1, \dots, n(N-k)$.

The computation of the i th component is as follows

$$\begin{aligned} \mathbf{x} \cdot \mathbf{h}_i^t &= \sum_{k=1}^n \sum_{j=0}^{N-1} h_{jn+k,i} \sigma_k(x_{j+1}) \\ &= \sum_{k=1}^n \sigma_k \left(\sum_{j=0}^{N-1} h_{jn+k,i} x_{j+1} \right) \\ &= \sigma_s \left(\sum_{j=1}^N h_{j,r}^c x_j \right) \\ &= \sigma_s(\tilde{\mathbf{x}} \cdot \mathbf{h}_r^c), \end{aligned}$$

where $r = \lfloor \frac{i}{n} \rfloor + 1$, $s = i - (r - 1)n$ and $\mathbf{h}_r^c = (h_{1,r}^c, \dots, h_{N,r}^c)^t$ is the r th column of \mathbf{H}^t . It should be noted that the two last equations in the above follows from the fact that \mathbf{h}_i is of the form $\mathbf{h}_i = (\mathbf{h}_i^1, \mathbf{h}_i^2, \dots, \mathbf{h}_i^N)^t$, where

$$\mathbf{h}_i^j = \left(\overbrace{0, \dots, 0}^{(s-1)\text{-times}}, h_{j,r}^c, \overbrace{0, \dots, 0}^{(n-s)\text{-times}} \right), \quad j = 1, \dots, N.$$

Thus

$$\begin{aligned} \mathbf{xH}_\Lambda^t &= (\sigma_1(\tilde{\mathbf{x}} \cdot \mathbf{h}_1^c), \dots, \sigma_n(\tilde{\mathbf{x}} \cdot \mathbf{h}_1^c), \dots, \\ &\quad \sigma_1(\tilde{\mathbf{x}} \cdot \mathbf{h}_{N-k}^c), \dots, \sigma_n(\tilde{\mathbf{x}} \cdot \mathbf{h}_{N-k}^c)) \\ &= (\sigma(\tilde{\mathbf{x}} \cdot \mathbf{h}_1^c), \dots, \sigma(\tilde{\mathbf{x}} \cdot \mathbf{h}_{N-k}^c)) \\ &= \sigma^{N-k}(\tilde{\mathbf{x}} \cdot \mathbf{h}_1^c, \dots, \tilde{\mathbf{x}} \cdot \mathbf{h}_{N-k}^c) \\ &= \sigma^{N-k}(\tilde{\mathbf{xH}}^t). \end{aligned}$$

Thus, $\rho((\sigma^{N-k})^{-1}(\mathbf{xH}_\Lambda^t)) = \mathbf{0}$ implies $\rho(\tilde{\mathbf{xH}}^t) = \mathbf{0}$ which indicates $\rho(\tilde{\mathbf{x}}) \in C$, and so $\mathbf{x} \in \Lambda$. ■

Theorem 7 is also valid in the non-binary case, where the conditions of Theorem 6 are fulfilled. The authors of [19] proposed Construction A based on number fields for non-binary linear codes. They have used cyclotomic number fields $\mathbb{Q}(\xi_{p^r})$ and their maximal totally real subfields $\mathbb{Q}(\xi_{p^r} + \xi_{p^r}^{-1})$, $r \geq 1$, as examples for their construction method. Using their method for the binary case $p = 2$ does not provide diversity and gives us the well known Construction A [2] that we describe in this section. In Section VI, we propose a new method for using Construction A over number fields in the binary case.

IV. MONOGENIC NUMBER FIELDS

In this section, we provide the required algebraic tools for developing Construction A lattices over a wider family of number fields: the monogenic number fields.

Definition 15: Let K be a number field of degree n and O_K be its ring of integers. If O_K , as a \mathbb{Z} -module, has a basis of the form $\{1, \alpha, \dots, \alpha^{n-1}\}$, for some $\alpha \in O_K$, then α is a *power generator*, the basis is a *power basis* and K is a *monogenic number field*.

It is a classical problem in algebraic number theory to identify if a number field K is monogenic or not. The quadratic and cyclotomic number fields are monogenic, but in general this is not the case. Dedekind [33, p. 64] was the first to notice this by giving an example of a

cubic field generated by a root of $t^3 - t^2 - 2t - 8$. The existence of a power generator simplifies the arithmetic in O_K . For instance, if K is monogenic, then the task of factoring pO_K into prime ideals over O_K , which is a difficult task in general, reduces to factoring the minimal polynomial of α over \mathbb{F}_p , which is significantly easier.

The proposed framework of [19] for developing Construction A lattices assumes that the number field K is a Galois extension of \mathbb{Q} . Therefore, our construction method based on monogenic number fields is not a special case of their method since there exist examples of number fields which are monogenic without being Galois extensions. For example let $K = \mathbb{Q}(\alpha)$, where $\alpha^3 = 2$ and α is the real cube root of 2. Then it is proved that $O_K = \mathbb{Z}[\alpha]$ [25, p. 67] and K is monogenic. However, it is known that $\mathbb{Q}(\sqrt[3]{2})$ is not a Galois extension.

We start by gathering the proved results about monogenic number fields and then we propose an algorithmic method to develop Construction A over monogenic number fields. We present the results about the number fields with degree less than 4. More details about monogenic number fields can be found in [34].

Theorem 8: [25, p. 76] Let m be a non-zero square-free integer and let $K = \mathbb{Q}(\sqrt{m})$. If $m \equiv 2$ or $3 \pmod{4}$, then $O_K = \mathbb{Z}[\sqrt{m}]$ is a basis for O_K over \mathbb{Z} . If $m \equiv 1 \pmod{4}$, then $O_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$.

Theorem 8 shows that all quadratic fields are monogenic. In the cubic case, however, these studies begin to get more complicated. In fact there are an infinite number of cyclic cubic fields which have a power basis and also an infinite number which do not, and similarly for quartic fields [35].

Let A be a Dedekind ring, K its quotient field, E a finite separable extension of K of degree n , and B the integral closure of A in E . Let $W = \{w_1, \dots, w_n\}$ be any set of n elements of E . The discriminant is

$$D_{E/K}(W) = \left(\det[\sigma_i(w_j)]_{i,j=1}^n \right)^2, \quad (26)$$

where σ_i 's are n distinct embeddings of E in a given algebraic closure of K . If M is a free module of rank n over A (contained in E), then we can define the discriminant of M by means of a basis of M over A . This notion is well defined up to the square of a unit in A .

Proposition 2: [25, p. 65] Let $M_1 \subset M_2$ be two free modules of rank n over A , contained in E . Then $D_{E/K}(M_1)$ divides $D_{E/K}(M_2)$. If $D_{E/K}(M_1) = uD_{E/K}(M_2)$ for some unit u of A , then $M_1 = M_2$.

It is useful to recall the following well-known result.

Lemma 1: [34, p. 1-2] Let K be a number field of degree n and $\alpha_1, \dots, \alpha_n \in O_K$ be linearly independent over \mathbb{Q} and set $Z_K = \mathbb{Z}[\alpha_1, \dots, \alpha_n]$. Then

$$D_{K/\mathbb{Q}}(\alpha_1, \dots, \alpha_n) = J^2 \cdot d_K,$$

where

$$J = [O_K^+ : Z_K^+],$$

O_K^+ and Z_K^+ are the additive groups of the corresponding modules and d_K is the discriminant of the field K .

Let $\alpha \in O_K$ be a primitive element of K , that is $K = \mathbb{Q}(\alpha)$. The index of α is defined by the module index

$$I(\alpha) = [O_K^+ : \mathbb{Z}[\alpha]^+]. \quad (27)$$

Obviously, α generates a power integral basis in K if and only if $I(\alpha) = 1$. The minimal index of the field K is defined by

$$\mu(K) = \min_{\alpha} I(\alpha),$$

where the minimum is taken over all primitive integers. The field index of K is

$$m(K) = \min_{\alpha} \gcd I(\alpha),$$

where the greatest common divisor is also taken over all primitive integers of K . Monogenic fields have both $\mu(K) = 1$ and $m(K) = 1$, but $m(K) = 1$ is not sufficient for being monogenic.

Let $\{1, \omega_2, \dots, \omega_n\}$ be an integral basis of K . Let

$$L(\mathbf{x}) = x_1 + x_2\omega_2 + \dots + x_n\omega_n,$$

with conjugates $L^{(i)}(\mathbf{x}) = x_1 + x_2\omega_2^{(i)} + \dots + x_n\omega_n^{(i)}$, where $\omega_j^{(i)} = \sigma_i(\omega_j)$, for $i, j = 1, \dots, n$.

The form $L(\mathbf{x}) = L(x_1, \dots, x_n)$ is the *fundamental form* and

$$D_{K/\mathbb{Q}}(L(\mathbf{x})) = \prod_{1 \leq i < j \leq n} (L^{(i)}(\mathbf{x}) - L^{(j)}(\mathbf{x}))^2$$

is the *fundamental discriminant*.

Lemma 2: [34, p. 2] We have

$$D_{K/\mathbb{Q}}(L(\mathbf{x})) = (I(x_2, \dots, x_n))^2 d_K, \quad (28)$$

where d_K is the discriminant of the field K and $I(x_2, \dots, x_n)$ is a homogeneous form in $n - 1$ variables of degree $n(n - 1)/2$ with integer coefficients. This form $I(x_2, \dots, x_n)$ is the index form corresponding to the integral basis $\{1, \omega_2, \dots, \omega_n\}$.

Lemma 3: For any primitive integer of the form $\alpha = x_1 + \omega_2 x_2 + \dots + \omega_n x_n \in O_K$ we have

$$I(\alpha) = |I(x_2, \dots, x_n)|.$$

Indeed, the existence of a power basis is equivalent to the existence of a solution to $I(x_2, \dots, x_n) = \pm 1$.

Theorem 9: [36, Theorem 7.1.8] Let K be an algebraic number field of degree n . Let $\alpha \in O_K$ be such that $K = \mathbb{Q}(\alpha)$. If $D_{K/\mathbb{Q}}(\alpha)$ is square-free, then $\{1, \alpha, \dots, \alpha^{n-1}\}$ is an integral basis for K . Indeed, K has a power integral basis.

The computation of the discriminant for some families of polynomials with small degree is a straightforward job. Combining these computations along with the conditions of Theorem 9 gives some useful results.

Theorem 10: [36, Theorems 7.1.10, 7.1.12, 7.1.15] Let a, b be integers such that

- 1) $x^3 + ax + b$ is irreducible. Let $\theta \in \mathbb{C}$ be a root of $x^3 + ax + b$ so that $K = \mathbb{Q}(\theta)$ is a cubic field and $\theta \in O_K$. Then $D_{K/\mathbb{Q}}(\theta) = -4a^3 - 27b^2$. If $D_{K/\mathbb{Q}}(\theta)$ is square-free or $D_{K/\mathbb{Q}}(\theta) = 4m$, where m is a square-free integer such that $m \equiv 2$ or $3 \pmod{4}$, then $\{1, \theta, \theta^2\}$ is an integral basis for the cubic field $\mathbb{Q}(\theta)$.
- 2) $x^4 + ax + b$ is irreducible. Let $\theta \in \mathbb{C}$ be a root of $x^4 + ax + b$ so that $K = \mathbb{Q}(\theta)$ is a quartic field and $\theta \in O_K$. Then $D_{K/\mathbb{Q}}(\theta) = -27a^4 + 256b^3$. If $D_{K/\mathbb{Q}}(\theta)$ is square-free, then $\{1, \theta, \theta^2, \theta^3\}$ is an integral basis for the quartic field $\mathbb{Q}(\theta)$.

Theorem 11: [36, p. 176] Let $K = \mathbb{Q}(\sqrt[3]{m})$, with $m \in \mathbb{Z}$ a cube-free number. Assume that $m = hk^2$ with $h, k > 0$ and hk is square-free, and let $\theta = m^{1/3}$. Then,

- for $m^2 \not\equiv 1 \pmod{9}$, we have $d_K = -27(hk)^2$, and the numbers $\{1, \theta, \theta^2/k\}$, form an integral basis of O_K ;
- for $m^2 \equiv \pm 1 \pmod{9}$, we have $d_K = -3(hk)^2$, and the numbers

$$\left\{ 1, \theta, \frac{k^2 \pm k^2 \theta + \theta^2}{3k} \right\},$$

form an integral basis of O_K .

This theorem shows that $\mathbb{Q}(\sqrt[3]{p})$ is monogenic for primes $p \equiv \pm 2, \pm 5 \pmod{9}$.

Let $a \in \mathbb{Z}$ be an arbitrary integer and consider a root ϑ of the polynomial

$$f(x) = x^3 - ax^2 + (a+3)x + 1. \quad (29)$$

Then, $K = \mathbb{Q}(\vartheta)$ are the *simplest cubic fields* [37]. This cubic equation has discriminant $D = (a^2 + 3a + 9)^2$ and if $a^2 + 3a + 9$ is prime, D is also the discriminant of the field $\mathbb{Q}(\vartheta)$. Accordingly, we have $\mathcal{O}_K = \mathbb{Z}[\vartheta]$ [37]. More information about monogenic number fields with higher degrees can be found in [34].

V. SYSTEM MODEL AND PERFORMANCE EVALUATION ON BLOCK-FADING CHANNELS

In this section, we describe the system models that describe communication over fading and block-fading channels using algebraic lattices. First, we describe communication over fading channels using algebraic lattices of the form $\sigma(\mathcal{O}_K)$ where K is a number field of degree n , \mathcal{O}_K the ring of integers of K and σ is the canonical embedding. We also present the available design criteria and performance measurements in fading channels. Then, by using Construction A lattices with an underlying (N, k) -linear code \mathcal{C} , this model is converted to a model that describes communication over a block-fading channel with fading block length N .

In communication over a flat fading channel, the received discrete-time signal vector is given by

$$\mathbf{y}_i = \mathbf{H}_F \mathbf{x}_i + \mathbf{z}_i, \quad i = 1, \dots, N, \quad (30)$$

where $\mathbf{y}_i \in \mathbb{R}^n$ is the received n -dimensional real signal vector, $\mathbf{x} \in \mathbb{R}^n$ is the transmitted n -dimensional real signal vector, $\mathbf{H}_F = \text{diag}(\mathbf{h})$ is an $n \times n$ real matrix, $\mathbf{h} = (h_1, \dots, h_n) \in \mathbb{R}^n$ is the flat fading diagonal matrix, and $\mathbf{z}_i \in \mathbb{R}^n$ is the noise vector whose samples are i.i.d. $\sim \mathcal{N}(0, \sigma^2)$. We define the signal-to-noise ratio (SNR) as $\rho = 1/\sigma^2$.

Let a frame be composed of N modulation symbols, each one with dimension n , or composed of nN channel uses. The case of complex signals obtained from 2 orthogonal real signals can be similarly modeled by (30) by replacing N with $N' = 2N$. In communication over a block-fading channel, we assume that the fading matrix \mathbf{H}_F is constant during one frame and it changes independently from frame to frame. This corresponds to a block-fading channel with n blocks [21]. We further assume perfect channel state information (CSI) at the receiver, i.e., the receiver perfectly knows the fading coefficients. Therefore, for a given fading realization, the channel transition probabilities are given by

$$p(\mathbf{y}|\mathbf{x}, \mathbf{H}_F) = (2\pi\sigma^2)^{-\frac{n}{2}} \exp\left(-\frac{1}{2\sigma^2} \|\mathbf{y} - \mathbf{H}_F \mathbf{x}\|^2\right). \quad (31)$$

Moreover, we assume that the real fading coefficients follow a Nakagami- m distribution

$$p_h(x) = \frac{2m^m x^{2m-1}}{\Gamma(m)} e^{-mx^2}, \quad (32)$$

where $m > 0$ and $\Gamma(x) \triangleq \int_0^{+\infty} t^{x-1} e^{-t} dt$ is the Gamma function. In the literature $m \geq 0.5$ is usually considered [38]; however, the fading distribution is well defined and reliable communication is possible for any $0 < m < 0.5$. Define the coefficients $\gamma_i = h_i^2$ for $i = 1, \dots, n$, which correspond to the fading power gains with probability density function (PDF) $p_\gamma(x) = \frac{m^m x^{m-1}}{\Gamma(m)} e^{-mx}$ and cumulative distribution function (CDF) $P_\gamma(x) = 1 - \bar{\Gamma}(mx, m)$, respectively, where $\bar{\Gamma}(a, x) \triangleq \frac{1}{\Gamma(a)} \int_x^{+\infty} t^{a-1} e^{-t} dt$ is the normalized incomplete Gamma function [39].

Analyzing the Nakagami- m fading channels, in which the fading coefficients have Nakagami- m distribution, recovers the analysis for other fading channels, including Rayleigh fading by setting $m = 1$ and Rician fading with parameter κ by setting $m = (\kappa + 1)^2 / (2\kappa + 1)$ [40].

A. Multidimensional lattice constellations

In communication using multidimensional constellations, the transmitted signal vectors \mathbf{x} belong to an n -dimensional signal constellation $\mathcal{S} \subset \mathbb{R}^n$. We consider signal constellations \mathcal{S} that are generated as a finite subset of points carved from the infinite lattice $\Lambda = \{\mathbf{u}\mathbf{M} + \mathbf{x}_0 | \mathbf{u} \in \mathbb{Z}^n\}$ with full rank generator matrix $\mathbf{M} \in \mathbb{R}^{n \times n}$ [2]. For a given channel realization, we define the faded lattice seen by the receiver as the lattice Λ' whose generator matrix is given by $\mathbf{M}' = \mathbf{H}_F \mathbf{M}$. In order to simplify the labeling operation, constellations are of the type $\mathcal{S} = \{\mathbf{M}\mathbf{u} + \mathbf{x}_0 | \mathbf{u} \in \mathbb{Z}_M^n\}$, where $\mathbb{Z}_M = \{0, 1, \dots, M-1\}$ represents an integer pulse-amplitude modulation (PAM) constellation, $\log_2(M)$ is the number of bits per dimension and \mathbf{x}_0 is an offset vector which minimizes the average transmitted energy. The rate of such constellations is $R = \log_2(M)$ bit/s/Hz. This is usually referred to as full-rate uncoded transmission [41].

B. Error performance of multidimensional lattice constellations over fading channels

The performance evaluation of multidimensional signal sets has attracted significant attention due to the signal space diversity (SSD) that these constellations present [42] and the fact that they can be efficiently used to combat the signal degradation caused by fading. The diversity order of a multidimensional signal set is the minimum number of distinct components between any two constellation points. In other words, the diversity order is the minimum Hamming distance between any two coordinate vectors of constellation points. To distinguish from other

well-known types of diversity (time, frequency, space, code) this type of diversity is called *modulation diversity* or *signal space diversity* (SSD) [42].

The design of such constellations has been extensively studied in [20], [41], [43], [44] and due to the difficulties in the analytical computation of the Voronoi cells of multidimensional constellations, their error performance has been evaluated only through approximations and bounds or only for specific lattice structures. The evaluation of multidimensional constellations can be done by considering the error performance of maximum likelihood (ML) decoder. At a given i , $1 \leq i \leq N$, a maximum likelihood decoder with perfect CSI makes an error whenever $\|\mathbf{y}_i - \mathbf{H}_F \mathbf{w}\|^2 \leq \|\mathbf{y}_i - \mathbf{H}_F \mathbf{x}_i\|^2$ for some $\mathbf{w} \in \mathcal{S}$, $\mathbf{w} \neq \mathbf{x}_i$. These inequalities define the so called decision region around \mathbf{x} . Under ML decoding, the frame error probability is then given by

$$P_f(\rho) = \mathbb{E}[P_f(\rho|\mathbf{h})] = \mathbb{E}[1 - (1 - P_s(\rho|\mathbf{h}))^N], \quad (33)$$

where \mathbf{h} consists of the diagonal elements of \mathbf{H}_F , and $P_f(\rho|\mathbf{h})$ and $P_s(\rho|\mathbf{h})$ are the frame and n -dimensional symbol error probabilities for a given channel realization and SNR ρ , respectively. The average is also taken over the fading distribution. For a given constellation \mathcal{S} , we have [41]

$$P_s(\rho|\mathbf{h}) = \mathbb{E}[P_s(\rho|\mathbf{x}, \mathbf{h})] = \frac{1}{|\mathcal{S}|} \sum_{\mathbf{x} \in \mathcal{S}} \int_{\mathbf{y} \notin \mathcal{V}(\mathbf{x}, \mathbf{h})} p(\mathbf{y}|\mathbf{x}, \mathbf{h}) d\mathbf{y},$$

where $\mathcal{V}(\mathbf{x}, \mathbf{h})$ is the decision region or Voronoi region for a given multidimensional lattice constellation point \mathbf{x} and fading \mathbf{H}_F . Computing the Voronoi regions and the exact error probability is in general a very hard problem. An sphere lower bound (SLB) on P_f has been proposed in [41]. The SLB dates back to Shannon's work [45] and it has been thoroughly investigated in the literature. However, it is not generally a reliable lower bound for the important practical cases of finite lattice constellations [44]. Therefore, another lower bound called multiple sphere lower bound (MSLB) is proposed in [44] in which the concept of the sphere lower bound is extended to the case of finite signal sets.

Definition 16: The diversity order is defined as the asymptotic (for large SNR) slope of P_f in a log-log scale, i.e.,

$$d \triangleq - \lim_{\rho \rightarrow \infty} \frac{\log P_f(\rho)}{\log \rho}. \quad (34)$$

The diversity order is usually a function of the fading distribution and the signal constellation \mathcal{S} . It is proved that the diversity order is the product of the signal space diversity and a parameter of the fading distribution [41].

Definition 17: A constellation $\mathcal{S} \subset \mathbb{R}^n$ has *full diversity* if the ML decoder is able to decode correctly in presence of $n - 1$ *deep fades*¹.

In this paper, our focus is on infinite lattices and we recall the basics of the sphere lower bound for infinite lattices \mathcal{S} [41], [46]. From the geometrical uniformity of lattices we have that $\mathcal{V}(\mathbf{x}, \mathbf{h}) = \mathcal{V}(\mathbf{w}, \mathbf{h}) = \mathcal{V}_\Lambda(\mathbf{h})$, for all $\mathbf{x}, \mathbf{w} \in \Lambda$. Therefore, we assume the transmission of the all-zero codeword, i.e., $\mathbf{x}_i = \mathbf{0}$, $i = 1, \dots, N$. Then, the error probability is given by [2]

$$P_f(\rho) = 1 - \mathbb{E} \left[\left(1 - \int_{\mathbf{z} \notin \mathcal{V}_\Lambda(\mathbf{h})} p(\mathbf{z}) d\mathbf{z} \right)^N \right]. \quad (35)$$

Due to the circular symmetry of the Gaussian noise, replacing $\mathcal{V}_\Lambda(\mathbf{h})$ by an n -dimensional sphere $\mathcal{B}(\mathbf{h})$ of the same volume and radius $R(\mathbf{h})$ [6], yields the corresponding sphere lower bound on the lattice performance [41], [46]

$$P_f(\rho) \geq P_{SLB}(\rho) = 1 - \mathbb{E} \left[\left(1 - \int_{\mathbf{z} \notin \mathcal{B}(\mathbf{h})} p(\mathbf{z}) d\mathbf{z} \right)^N \right]. \quad (36)$$

In [41], for normalization purposes, it is assumed that $\det(M) = 1$ and sphere lower bound is obtained for normalized lattices. Here we present the sphere lower bound without this assumption. Equating the volume of $\mathcal{B}(\mathbf{h})$ which is [2]

$$\text{vol}(\mathcal{B}(\mathbf{h})) = \frac{\pi^{\frac{n}{2}} R(\mathbf{h})^n}{\Gamma\left(\frac{n}{2} + 1\right)},$$

to the fundamental volume of the lattice given by $\text{vol}(\mathcal{V}_\Lambda(\mathbf{h})) = \det(\mathbf{H}_F \mathbf{M}) = \det(M) \prod_{i=1}^n h_i$ yields the sphere radius

$$R(\mathbf{h})^2 = \frac{1}{\pi} \left(\Gamma\left(\frac{n}{2} + 1\right) \det(M) \prod_{i=1}^n h_i \right)^{\frac{2}{n}}. \quad (37)$$

The probability that the noise brings the received point outside the sphere $\mathcal{B}(\mathbf{h})$ is expressed as [41], [45], [46]

$$P_{SLB}(\rho) = 1 - \mathbb{E} \left[\left(1 - \bar{\Gamma}\left(\frac{n}{2}, \frac{R(\mathbf{h})^2}{2} \rho\right) \right)^N \right]. \quad (38)$$

¹When the transmitter and receiver are surrounded by reflectors, a transmitted signal can traverse in multiple paths and the receiver sees the superposition of multiple copies of the transmitted signal with different attenuations, delays and phase shifts. This can result in either constructive or destructive interference, amplifying or attenuating the signal power of the receiver. Strong destructive interference is frequently referred to as a deep fade and may result in temporary failure of communication due to a severe drop in the channel signal-to-noise ratio.

C. Optimal lattice constellations

We need an estimate of the error probability of the above system to address the search for good constellations. Consider the multidimensional constellation $\mathcal{S} \subset \Lambda$. Due to the geometrically uniformity of the lattice, we may simply write $P_e(\Lambda) = P_e(\Lambda|\mathbf{x})$ for any transmitted point $\mathbf{x} \in \Lambda$. Thus, \mathbf{x} can be considered as the all zero vector. By applying the union bound and taking into account the edge effects of the finite constellation \mathcal{S} compared to the infinite lattice Λ , we obtain an upper bound to the point error probability [43]

$$P_e(\mathcal{S}) \leq P_e(\Lambda) \leq \sum_{\mathbf{x} \neq \mathbf{w}} P(\mathbf{x} \rightarrow \mathbf{w}), \quad (39)$$

where $P(\mathbf{x} \rightarrow \mathbf{w})$ is the pairwise error probability, the probability that the received point \mathbf{y} is closer to \mathbf{w} than to \mathbf{x} according to the metric

$$m(\mathbf{x}|\mathbf{y}, \mathbf{h}) = \sum_{i=1}^n |y_i - h_i x_i|^2, \quad (40)$$

when \mathbf{x} is transmitted. In [43], using the Chernoff bounding technique, it is shown that

$$P(\mathbf{x} \rightarrow \mathbf{w}) \leq \frac{1}{2} \prod_{x_i \neq w_i} \frac{4\sigma^2}{(x_i - w_i)^2} = \frac{(4\sigma^2)^\ell}{2d_p^{(\ell)}(\mathbf{x}, \mathbf{w})^2}, \quad (41)$$

where $\ell = |\{1 \leq i \leq n | x_i \neq w_i\}|$. Let us define $L = \min_{\mathbf{x} \neq \mathbf{w} \in \mathcal{S}} \{\ell\}$ as the diversity order. Thus, the point error probability of a multidimensional signal set is essentially dominated by four factors and to improve performance it is necessary to [43]

- 1) minimize the average energy per constellation point;
- 2) maximize the signal space diversity L ;
- 3) maximize the minimum L -product distance

$$d_{p,\min}^{(L)} = \prod_{x_i \neq y_i}^L |x_i - y_i| \quad (42)$$

between any two points \mathbf{x} and \mathbf{y} in the constellation;

- 4) minimize the product kissing number τ_p for the L -product distance, i.e., the total number of points at the minimum L -product distance.

To minimize the error probability, one should maximize the diversity order L , i.e., have full diversity $L = n$. Algebraic lattices of the form $\sigma(O_K)$, where O_K is the integers ring of a number field K , have diversity order $r_1 + r_2$, where (r_1, r_2) is the signature of K [20]. Therefore, totally real algebraic lattices have full diversity. On the other hand, the rank of a lattice determines the

number of vectors we get with a given power limit and smaller rank means less constellation vectors. Hence, it is preferable to look at full rank lattices. Next, we should decide which one of the full rank lattices has the biggest minimum product distance. For two lattices with the same minimum product distance, the one with smaller parallelotope has better performance. Due to Theorem 5, in order to minimize the volume of algebraic lattices it suffices to minimize the discriminant.

D. Poltyrev outage limit for lattices

In the preceding subsections, we introduced the evaluation methods for finite multidimensional constellations, including lattice constellations. In order to evaluate infinite lattices over the AWGN channels [32], we usually employ Poltyrev limit [3]. Due to this limit, there exists a lattice Λ , with generator \mathbf{G}_Λ , of high enough dimension n for which the transmission error probability over the AWGN channel decreases to an arbitrary low value if and only if $\sigma^2 < \sigma_{max}^2$, where σ^2 is the noise variance per dimension, and σ_{max}^2 is the Poltyrev threshold which is given by

$$\sigma_{max}^2 = \frac{|\det(\mathbf{G}_\Lambda)|^{\frac{2}{n}}}{2\pi e}. \quad (43)$$

Using Poltyrev threshold, a *Poltyrev outage limit* for lattices over block-fading channels is proposed in [23]. It is proved that Poltyrev outage limit has diversity L for a channel with L independent block fading, i.e., Poltyrev outage limit has full diversity [23]. Using our notations through this paper, for a fixed instantaneous fading $\mathbf{h} = (h_1, \dots, h_n)$, Poltyrev threshold becomes [23]

$$\sigma_{max}^2(\mathbf{h}) = \frac{|\det(\mathbf{G}_\Lambda)|^{\frac{2}{nN}} \prod_{i=1}^n h_i^{\frac{2}{n}}}{2\pi e}. \quad (44)$$

The decoding of the lattice with generator \mathbf{G}_Λ is possible with a vanishing error probability if $\sigma^2 < \sigma_{max}^2(\mathbf{h})$ [3], [23]. Thus, for variable fading, an outage event occurs whenever $\sigma^2 > \sigma_{max}^2(\mathbf{h})$. The Poltyrev outage limit $P_{out}(\rho)$ is defined as follows [23]

$$\begin{aligned} P_{out}(\rho) &= \Pr \left(\sigma^2 > \frac{|\det(\mathbf{G}_\Lambda)|^{\frac{2}{nN}} \prod_{i=1}^n h_i^{\frac{2}{n}}}{2\pi e} \right) \\ &= \Pr \left(\prod_{i=1}^n h_i^2 < \frac{(2\pi e)^n}{|\det(\mathbf{G}_\Lambda)|^{\frac{2}{N}} \rho^n} \right), \end{aligned} \quad (45)$$

where $|\det(\mathbf{G}_\Lambda)| = 2^{nN+N-k} d_K^{\frac{N}{2}}$ for our lattices. The closed-form expression of $P_{out}(\rho)$ is not derived in [23]; however it can be estimated numerically via Monte Carlo simulation. For a given

lattice, the frame error rate after lattice decoding over a block-fading channel, can be compared to $P_{out}(\rho)$ to measure the gap in SNR and verify the diversity order.

VI. CONSTRUCTION A OVER MONOGENIC NUMBER FIELDS

In this section we give more precise information concerning the splitting of the primes over monogenic number fields that helps us to develop Construction A lattices over monogenic number fields.

Proposition 3: [25, p. 27] Let A be a Dedekind ring with quotient field K . Let E be a finite separable extension of K . Let B be the integral closure of A in E and assume that $B = A[\alpha]$ for some element α . Let f be the irreducible polynomial of α over K and let \mathfrak{p} be a prime of A . Consider \bar{f} to be the reduction of $f \pmod{\mathfrak{p}}$, and let

$$\bar{f}(x) = \bar{P}_1(x)^{e_1} \cdots \bar{P}_r(x)^{e_r}, \quad (46)$$

be the factorization of \bar{f} into powers of irreducible factors over $\bar{A} = A/\mathfrak{p}$. Then

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \quad (47)$$

is the factorization of \mathfrak{p} in B , so that e_i is the ramification index of \mathfrak{P}_i over \mathfrak{p} , and we have

$$\mathfrak{P}_i = \mathfrak{p}B + P_i(\alpha)B, \quad (48)$$

where $P_i \in A[x]$ is a polynomial with leading coefficient 1 whose reduction mod \mathfrak{p} is \bar{P}_i . For each i , \mathfrak{P}_i has residue class degree $[B/\mathfrak{P}_i : A/\mathfrak{p}] = d_i$, where $d_i = \deg(\bar{P}_i)$.

In our case, $A = \mathbb{Z}$, $K = \mathbb{Q}$, $E = \mathbb{Q}(\alpha)$, $B = O_E = \mathbb{Z}[\alpha]$ and $\mathfrak{p} = 2\mathbb{Z}$. Let f be the minimal polynomial of α over \mathbb{Q} and $\bar{f} = f \pmod{2}$. Write the decomposition of \bar{f} in $\mathbb{F}_2[x]$ as follows

$$\bar{f}(x) = \bar{P}_1(x)^{e_1} \cdots \bar{P}_r(x)^{e_r}.$$

Then, we have

$$2O_E = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

where $\mathfrak{P}_j = 2O_E + P_j(\alpha)O_E$, for $j = 1, \dots, r$. If there exists \bar{P}_i such that $d_i = \deg(\bar{P}_i) = 1$ then $O_E/\mathfrak{P}_i \simeq \mathbb{F}_2$. Now, we can define the map $\rho : O_E^N \rightarrow \mathbb{F}_2^N$ as componentwise reduction modulo \mathfrak{P}_i and develop the Construction A lattice $\Gamma_{\mathcal{C}} = \rho^{-1}(\mathcal{C})$ for an (N, k) linear code \mathcal{C} .

As the simplest case, we present our method for block-fading channels with two fading blocks, i.e., $n = 2$. We require quadratic fields of the form $K = \mathbb{Q}(\sqrt{m})$, where m is a positive square-free integer; these fields are totally real. Theorem 8 determines the structure of O_K for these number fields.

Theorem 12: Let $K = \mathbb{Q}(\sqrt{m})$. Then, $2\mathcal{O}_K$ is totally ramified with $2\mathcal{O}_K \cong \mathfrak{P}^2$ when $m \equiv 2 \pmod{4}$ and $\mathfrak{P} = 2\mathbb{Z}[\sqrt{m}] + \sqrt{m}\mathbb{Z}[\sqrt{m}]$, or $m \equiv 3 \pmod{4}$, $\mathfrak{P} = 2\mathbb{Z}[\sqrt{m}] + (\sqrt{m}+1)\mathbb{Z}[\sqrt{m}]$. In both of these cases we have $\mathcal{O}_K/\mathfrak{P} \cong \mathbb{F}_2$. If $m \equiv 1 \pmod{4}$, then $2\mathcal{O}_K$ is not totally ramified, but if $(m-1)/4$ is an even number, then $2\mathcal{O}_K \cong \mathfrak{P}_1\mathfrak{P}_2$ and $\mathcal{O}_K/\mathfrak{P}_i \cong \mathbb{F}_2$, $i = 1, 2$, where $\mathfrak{P}_1 = 2\mathbb{Z}[\alpha] + \alpha\mathbb{Z}[\alpha]$ and $\mathfrak{P}_2 = 2\mathbb{Z}[\alpha] + (\alpha+1)\mathbb{Z}[\alpha]$, with $\alpha = (1 + \sqrt{m})/2$.

Proof: All quadratic fields of the form $\mathbb{Q}(\sqrt{m})$, where m is a positive square-free integer, are monogenic and totally real. If $m \equiv 2$ or $3 \pmod{4}$, then $\alpha = \sqrt{m}$ is the generator of the power integral basis with minimal polynomial $f(x) = x^2 - m$. In this case, f always has a linear factor after reduction modulo 2. Indeed, we have $\bar{f}(x) = x^2$ for even m 's and $\bar{f}(x) = (x+1)^2$ for odd m 's. If $m \equiv 1 \pmod{4}$ then $\alpha = (1 + \sqrt{m})/2$ is the generator of power integral basis with minimal polynomial $f(x) = x^2 - x - (m-1)/4$. It can be easily seen that in this case, f has a linear factor after reduction modulo 2 if and only if $(m-1)/4$ is an even number, i.e., $m \equiv 1 \pmod{8}$. In this case, $\bar{f}(x) = x(x+1)$. The rest of the proof follows from Proposition 3. ■

In all cases of Theorem 12, there is at least one prime ideal \mathfrak{P}_i in \mathcal{O}_K such that $\mathcal{O}_K/\mathfrak{P}_i \cong \mathbb{F}_2$. Define the map $\rho : \mathcal{O}_K^N \rightarrow \mathbb{F}_2^N$ as componentwise reduction modulo \mathfrak{P}_i and implement the Construction A lattice $\Gamma_{\mathcal{C}} = \rho^{-1}(\mathcal{C})$ for an (N, k) binary LDPC code \mathcal{C} . Then, $\Lambda = \sigma^N(\Gamma_{\mathcal{C}})$ is a 1-level LDPC lattice of diversity order 2 in \mathbb{R}^{2N} .

Example 2: We have seen that the simplest cubic fields $K = \mathbb{Q}(\vartheta)$ where ϑ is a root of the polynomial $f(x) = x^3 - ax^2 + (a+3)x + 1$, is a totally real monogenic number field, when $a^2 + 3a + 9$ is a prime number. Even though this condition holds, these families of number fields are useless for our case since for each $a \in \mathbb{Z}$, $x^3 - ax^2 + (a+3)x + 1 \pmod{2}$ is one of the polynomials $x^3 + x^2 + 1$ or $x^3 + x + 1$ and both of these polynomials are irreducible over \mathbb{F}_2 .

Another examples are $K = \mathbb{Q}(\theta)$ where θ has minimal polynomial of the form $x^3 + ax + b$. In this case, if $-4a^3 - 27b^2$ or $(-4a^3 - 27b^2)/4$ are square free then K is monogenic. For example put $a = 3$ and $b = 2$. Then $-4a^3 - 27b^2 = -4 \cdot 59$ which is a square-free integer after dividing by 4. Hence, $K = \mathbb{Q}(\theta)$ where $f(\theta) = \theta^3 + 3\theta + 2 = 0$ is a monogenic number field. We have

$$\bar{f}(x) = x^3 + x = x(x+1)^2.$$

Due to this factorization, each one of the primes $\mathfrak{P}_1 = 2\mathbb{Z}[\theta] + 2\theta\mathbb{Z}[\theta]$ or $\mathfrak{P}_2 = 2\mathbb{Z}[\theta] + 2(\theta+1)\mathbb{Z}[\theta]$ gives us $\mathcal{O}_K/\mathfrak{P}_i \cong \mathbb{F}_2$. It can be easily checked that $\mathbb{Q}(\theta)$ is not totally real which is the only problem about these family of cubic polynomials.

Pure cubic fields of the form $\mathbb{Q}(\sqrt[3]{p})$ are monogenic for primes $p \equiv \pm 2, \pm 5 \pmod{9}$. In this case the factorization of $x^3 - p$ always has a linear factor. Unfortunately, all pure cubic fields are complex. \square

In the existing number fields of degree 3, we did not find any parametric family for which both being totally real and having linear factor after reduction modulo 2 hold. There are a lot of numerical studies for finding monogenic number fields. An excellent account is provided in the tables of [34, Section 11] containing all generators of power integral bases for 130 cubic fields with small discriminants (both positive and negative), cyclic quartic, totally real and totally complex biquadratic number fields up to discriminants 10^6 and 10^4 , respectively. Furthermore, the five totally real cyclic sextic fields with smallest discriminants, the 25 sextic fields with an imaginary quadratic subfield with smallest absolute value of discriminants and their generators of power integral bases are also given in [34].

We could generate many examples of number fields with different degrees of which the aforementioned two conditions are fulfilled. We used SAGE [47] to generate these examples but most of these results were already included in [34]. Let us analyse the results of [34] about totally real cubic fields.

The provided table in [34, Tabel 11.1.1] contains all power integral bases of totally real cubic fields of discriminants $49 \leq d_K \leq 3137$. The rows contain the following data: d_K , (a_1, a_2, a_3) , where d_K is the discriminant of the field K , generated by a root ϑ of the polynomial $f(x) = x^3 + a_1x^2 + a_2x + a_3$, and (I_0, I_1, I_2, I_3) coefficients of the index form equation. In most of these fields $\{1, \omega_2 = \vartheta, \omega_3 = \vartheta^2\}$ is an integral basis; if not, then an integral basis is given by $\{1, \omega_2, \omega_3\}$ with $\omega_2 = (p_0 + p_1\vartheta + p_2\vartheta^2)/p$, $\omega_3 = (q_0 + q_1\vartheta + q_2\vartheta^2)/q$ and the table includes the coefficients $\omega_2 = (p_0, p_1, p_2)/p$, $\omega_3 = (q_0, q_1, q_2)/q$. Finally, the solutions (x, y) , of the index form equation are displayed. All generators of power integral bases of the field K are of the form

$$\alpha = a \pm (x\omega_2 + y\omega_3),$$

where $a \in \mathbb{Z}$ is arbitrary and (x, y) is a solution of the index form equation. For $\overline{a_i} \equiv a_i \pmod{2}$, $1 \leq i \leq 3$, the polynomial f admits a linear factor after reduction modulo 2, in one of the following cases

- 1) $\overline{a_3} = 0$;
- 2) $\overline{a_1} \neq 0$ and $\overline{a_2} = \overline{a_3} = 0$;

3) $\overline{a_1} \neq 0$, $\overline{a_2} \neq 0$ and $\overline{a_3} \neq 0$.

Consequently, for the following values of discriminant in [34, Table 11.1.1], we obtain a full diversity Construction A lattice with binary linear codes as underlying code

148, 229, 316, 404, 469, 564, 568, 621, 733, 756,
 788, 837, 892, 940, 1016, 1076, 1101, 1229, 1300, 1373,
 1384, 1396, 1436, 1492, 1524, 1556, 1573, 1620, 1708, 1765,
 1901, 1940, 1944, 1957, 2021, 2024, 2101, 2213, 2296, 2300,
 2349, 2557, 2597, 2677, 2700, 2708, 2804, 2808, 2836, 2917,
 2981, 3021, 3028,

which is 53/93 or 57% of the cases.

Example 3: Consider the number field $K = \mathbb{Q}(\nu)$, where ν is the root of the polynomial $f(x) = ax^3 + bx^2 + cx + d = x^3 - x^2 - 3x + 1$. Due to the above discussion, K is monogenic with $d_K = 148$ and $\mathcal{O}_K = \mathbb{Z}[\nu]$. Since the discriminant of f , which is $\Delta = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2 = 148$, is positive f has 3 real roots as follows

$$\begin{aligned} x_1 &= \frac{-1}{3} \left(-1 + \zeta^0 C + \frac{\Delta_0}{\zeta^0 C} \right) = -1.4812, \\ x_2 &= \frac{-1}{3} \left(-1 + \zeta^1 C + \frac{\Delta_0}{\zeta^1 C} \right) = 2.170086, \\ x_3 &= \frac{-1}{3} \left(-1 + \zeta^2 C + \frac{\Delta_0}{\zeta^2 C} \right) = 0.311107, \end{aligned}$$

in which $\Delta_0 = b^2 - 3ac$, $\zeta = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ and

$$C = \sqrt[3]{\frac{\Delta_1 \pm \sqrt{\Delta_1^2 - 4\Delta_0^3}}{2}}, \quad \Delta_1 = 2b^3 - 9abc + 27a^2d.$$

The integral basis of K is generated by $\nu = x_1$ as $\{1, \nu, \nu^2\}$ and using the embeddings σ_1 that sends x_1 to x_1 , σ_2 that sends x_1 to x_3 and σ_3 that sends x_1 to x_2 , gives us

$$\mathbf{M} = \begin{bmatrix} 1 & 1 & 1 \\ x_1 & x_3 & x_2 \\ x_1^2 & x_3^2 & x_2^2 \end{bmatrix},$$

as the generator matrix of the lattice $\sigma(\mathcal{O}_K)$. Decomposing $\overline{f}(x) = f(x) \pmod{2} = x^3 + x^2 + x + 1$ as $(x+1)^3$ admits the following decomposition

$$2\mathcal{O}_K = \mathfrak{P}^3, \quad \frac{\mathcal{O}_K}{\mathfrak{P}} \cong \mathbb{F}_2,$$

where $\mathfrak{P} = 2\mathcal{O}_K + (x_1 + 1)\mathcal{O}_K$ is a prime ideal of \mathcal{O}_K . It can be checked that $\{2, x_1 + 1, x_1^2 - x_1 - 2\}$ is a \mathbb{Z} -basis for \mathfrak{P} . Thus, the generator matrix of the lattice $\sigma(\mathfrak{P})$ is

$$\mathbf{DM} = \begin{bmatrix} 2 & 2 & 2 \\ x_1 + 1 & x_3 + 1 & x_2 + 1 \\ x_1^2 - x_1 - 2 & x_3^2 - x_3 - 2 & x_2^2 - x_2 - 2 \end{bmatrix}.$$

Now, we consider an $[N, k]$ -LDPC code with parity check matrix \mathbf{H}_C and generator matrix $\mathbf{G}_C = \begin{bmatrix} \mathbf{I}_k & \mathbf{A} \end{bmatrix}$ that gives us the parity check and generator matrices of the triple diversity 1-level LDPC lattice $\Lambda = \sigma^N(\Gamma_C)$ as \mathbf{M}_Λ and \mathbf{H}_Λ in Theorem 7, respectively. \square

Example 4: Next, we analyze the totally real quartic number fields. First examples of such fields are simplest quartic fields which had power integral in only two cases; see [34]. These two cases are $K_2 = \mathbb{Q}(\vartheta_2)$ and $K_4 = \mathbb{Q}(\vartheta_4)$ where ϑ_2 is a root of $f(x) = x^4 - 2x^3 - 6x^2 + 2x + 1$ and ϑ_4 is a root of $f(x) = x^4 - 4x^3 - 6x^2 + 4x + 1$. The integral bases and solutions of index form equations with respect to these bases have been presented in [34]. Let $\{1, \omega_1, \omega_2, \omega_3\}$ represent the integral bases of K_2 and K_4 . The generators of the power integral basis of K_2 and K_4 are of the form $\alpha = a + x_1\omega_1 + x_2\omega_2 + x_3\omega_3$, where $a \in \mathbb{Z}$ is arbitrary and (x_1, x_2, x_3) is a solution of the corresponding index form equations of K_2 and K_4 . For each α of this form we need to find its minimal polynomial over \mathbb{Q} to check whether its reduction modulo 2 has linear factors or not. The minimal polynomials have been computed using SAGE [47] and are presented in TABLE I and TABLE II for K_2 and K_4 , respectively. We have that the minimal polynomials of the power generators of K_2 are equivalent to $t^4 + t^2 + 1$ modulo 2 which has no linear factor. For K_4 , all of them are equivalent to either t^4 or $t^4 + 1$ which have linear factors. It can be shown that $d_{K_2} = 2000$ and $d_{K_4} = 2048$.

Totally real bicyclic biquadratic number fields are other examples. Using the algorithm described in [34, Section 6.5.2], the minimal index $\mu(K)$ and all elements with minimal index in the 196 totally real bicyclic biquadratic number fields $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ with discriminant smaller than 10^6 have been determined. The results are gathered in [34, Table 11.2.5]. In this table, the solutions of index form equation $I(x_2, x_3, x_4) = \mu(K)$ has been proposed. The cases with $\mu(K) = 1$ are the cases that K has power integral basis. In the cases that K has a power integral basis with power generator α , we have computed the minimal polynomial and the results are summarized in TABLE III. \square

More quartic fields with certain signatures and Galois groups are computed and gathered in [34, Section 11.2.7]. The tables in [34, Section 11.2.7] contain the following data. In the first

TABLE I
MINIMAL POLYNOMIALS OF SIMPLEST QUARTIC FIELDS FOR $a = 2$.

(x_1, x_2, x_3)	Minimal Polynomial
$(0, 1, 0)$	$t^4 - 10t^3 + 25t^2 - 20t + 5$
$(-1, 1, 0)$	$t^4 - 8t^3 + 19t^2 - 12t + 1$
$(6, 5, -2)$	$t^4 - 22t^3 + 169t^2 - 508t + 421$
$(0, 4, -1)$	$t^4 - 20t^3 + 115t^2 - 260t + 205$
$(-12, -4, 3)$	$t^4 - 4t^3 - 29t^2 - 44t - 19$
$(-8, -3, 2)$	$t^4 + 6t^3 + t^2 - 4t - 1$
$(1, 1, 0)$	$t^4 - 12t^3 + 19t^2 - 8t + 1$
$(-2, 1, 0)$	$t^4 - 6t^3 + t^2 + 4t + 1$
$(-13, -9, 4)$	$t^4 + 36t^3 + 451t^2 + 2176t + 2641$
$(4, 2, -1)$	$t^4 - 8t^3 + 19t^2 - 12t + 1$

TABLE II
MINIMAL POLYNOMIALS OF SIMPLEST QUARTIC FIELDS FOR $a = 4$.

(x_1, x_2, x_3)	Minimal Polynomial
$(3, 2, -1)$	$t^4 - 4t^3 + 2t^2 + 4t - 1$
$(-2, -2, 1)$	$t^4 - 8t^2 - 8t - 2$
$(4, 8, -3)$	$t^4 - 24t^3 + 208t^2 - 760t + 958$
$(-6, -7, 3)$	$t^4 + 16t^3 + 88t^2 + 200t + 158$
$(0, 3, -1)$	$t^4 - 8t^3 + 16t^2 - 8t - 2$
$(1, 3, -1)$	$t^4 - 12t^3 + 50t^2 - 84t + 47$

column the discriminant of the field $K = \mathbb{Q}(\xi)$, the second column contains the coefficients (a_1, a_2, a_3, a_4) of the minimal polynomial $f_\xi(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ of ξ . In the third column the minimal m for which the index form equation $I(x_2, x_3, x_4) = \pm m$ has solutions with $|x_2|, |x_3|, |x_4| < 10^{10}$. It is followed by an integral basis of K in case the integral basis is not the

TABLE III
MONOGENIC TOTALLY REAL BICYCLIC BIQUADRATIC NUMBER FIELDS.

d_K	m	n	$l = (m, n)$	α	Minimal Polynomial f_α	Linear factor in $\overline{f_\alpha}$
2304	2	3	1	$\frac{\sqrt{2}+\sqrt{6}}{2}$	$t^4 - 4t^2 + 1$	Yes
7056	7	3	1	$\frac{\sqrt{7}+\sqrt{3}}{2}$	$t^4 - 5t^2 + 1$	No
24336	39	3	3	$-\sqrt{39} + 2\frac{\sqrt{39}+\sqrt{3}}{2} + \frac{1+\sqrt{13}}{2}$	$t^4 - 2t^3 - 11t^2 + 12t - 3$	No
57600	6	15	3	$\frac{\sqrt{6}+\sqrt{10}}{2}$	$t^4 - 8t^2 + 1$	Yes
94846	11	7	1	$\frac{\sqrt{11}+\sqrt{7}}{2}$	$t^4 - 9t^2 + 1$	No
313600	10	35	5	$\frac{\sqrt{10}+\sqrt{14}}{2}$	$t^4 - 12t^2 + 1$	Yes
435600	15	11	1	$\frac{\sqrt{11}+\sqrt{15}}{2}$	$t^4 - 13t^2 + 1$	No
659344	203	7	7	$-\sqrt{203} + 2\frac{\sqrt{203}+\sqrt{7}}{2} + \frac{1+\sqrt{203}}{2}$	$t^4 - 2t^3 - 27t^2 + 28t - 7$	No

power basis. Last column contains the solutions (x_2, x_3, x_4) with absolute values smaller than 10^{10} of the index form equation $I(x_2, x_3, x_4) = \pm m$. We have collected the cases that $\mathbb{Q}(\xi)$ has a power integral basis and f_ξ admits a linear factor after reduction modulo 2. We have presented these cases by their discriminants in the following lists:

1) totally real quartic fields with Galois group A_4

26569, 33489, 121801, 165649, 261121, 270400, 299209,
346921, 368449, 373321, 408321, 423801, 473344,
502681, 529984, 582169, 660969, 877969;

2) totally real quartic fields with Galois group S_4

2777, 6224, 6809, 7537, 8468, 10273, 10889, 11324,
11344, 11348, 13676, 13768, 14656, 15188, 15529, 15952.

VII. DECODING OF FULL DIVERSITY 1-LEVEL LDPC LATTICES

In this section we propose a new decoder, which is based on sum-product algorithm of LDPC codes and sphere decoder [48] of low dimensional lattices, for full diversity 1-level LDPC lattices. We also analyze the decoding complexity of the proposed algorithm.

Let \mathcal{C} be an (N, k) -LDPC code and O_K be the integers ring of a totally real number field K of degree n . Let \mathfrak{p} be a prime ideal of O_K such that $O_K/\mathfrak{p} \simeq \mathbb{F}_2$. Also, consider $\sigma_1, \dots, \sigma_n$ to be n real embeddings of K . Every lattice vector \mathbf{x} in $\sigma^N(\Gamma_{\mathcal{C}}) = \sigma^N(\rho^{-1}(\mathcal{C}))$ has the following form

$$\begin{aligned}
\mathbf{x} &= \sigma^N(\mathbf{c} + \mathbf{p}) \\
&= (\sigma(c_1 + p_1), \dots, \sigma(c_N + p_N)) \\
&= (\sigma_1(c_1 + p_1), \dots, \sigma_n(c_1 + p_1), \dots, \sigma_n(c_N + p_N)) \\
&= (c_1 + \sigma_1(p_1), \dots, c_1 + \sigma_n(p_1), \dots, c_N + \sigma_n(p_N)) \\
&= \mathbf{c} \otimes \underbrace{(1, \dots, 1)}_{n\text{-times}} + \sigma^N(\mathbf{p}), \tag{49}
\end{aligned}$$

where \otimes is the Kronecker product, $\mathbf{c} \in \mathcal{C}$ and $\mathbf{p} \in \mathfrak{p}^N$. To simulate the operation of our decoding algorithm, we use Rayleigh block-fading channel model; see Section V. Rayleigh fading is a reasonable model when there are many objects in the environment that scatter the radio signal before it arrives at the receiver. Due to the central limit theorem, if there is sufficiently much scatter, the channel impulse response is modelled as a Gaussian process. If the scatters have no dominant components, then such a process will have zero mean and phase evenly distributed between 0 and 2π radians. Thus, the envelope of the channel response is Rayleigh distributed. Often, the gain and phase elements of such channel's distortion are represented as complex numbers. In this case, Rayleigh fading is exhibited by a complex random variable with real and imaginary parts modelled by independent and identically distributed zero-mean Gaussian processes. With the aid of an in-phase/quadrature component interleaver [19], [20], it is possible to remove the phase of the complex fading coefficients to obtain a real fading which is Rayleigh distributed and guarantee that the fading coefficients are independent from one real symbol to the next.

Let \mathbf{y} be the received vector from Rayleigh block-fading channel with n fading blocks and coherence time N

$$\mathbf{y}^t = (\mathbf{I}_N \otimes \mathbf{H}_{\mathbf{F}})\mathbf{x}^t + \mathbf{n}^t, \tag{50}$$

where $\mathbf{H}_{\mathbf{F}} = \text{diag}(|h_1|, \dots, |h_n|)$ and the fading coefficients h_i are complex Gaussian random variables with variance σ_b^2 , so that $|h_i|$ are Rayleigh distributed with parameter σ_b^2 , for all $i = 1, \dots, n$, and $\mathbf{n} = (\nu_1, \dots, \nu_{nN})$, where $\nu_i \sim \mathcal{N}(0, \sigma^2)$ is the Gaussian noise, for $i = 1, \dots, nN$.

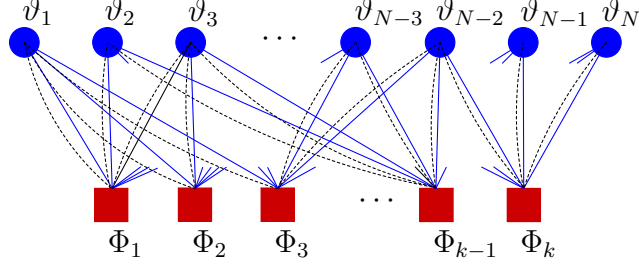


Fig. 1. Tanner graph for a full-diversity 1-level LDPC lattice with regular $(3, 6)$ LDPC code as underlying code.

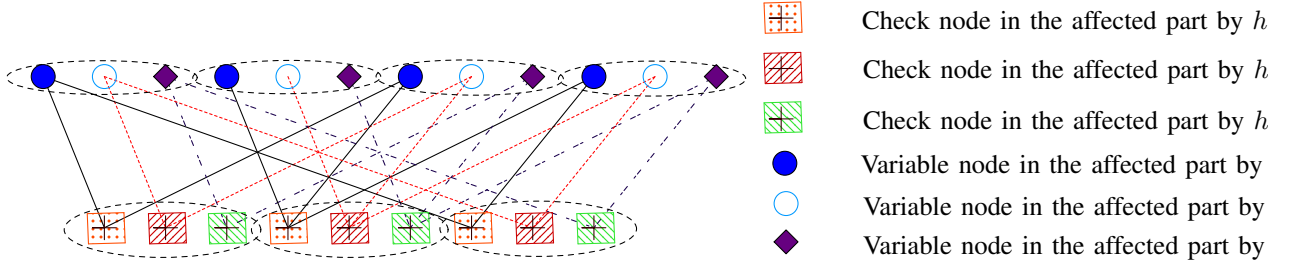


Fig. 2. Notation and diagram for the Tanner graph of a full diversity 1-level LDPC lattice for a block-fading channel with 3 fading blocks.

To simplify our decoding algorithm, we use the scaled and translated version of $\sigma^N(\Gamma_C)$ [2, §20.5], [7]. Hence, instead of \mathbf{x} , we use $\mathbf{x}' = 2\mathbf{x} - (1, \dots, 1)$ as transmitted vector. Now, the received vector is

$$\mathbf{y}^t = (\mathbf{I}_N \otimes \mathbf{H}_F) \mathbf{x}^t + \mathbf{n}^t = 2(\mathbf{I}_N \otimes \mathbf{H}_F) \mathbf{x}' - (1, \dots, 1)^t + \mathbf{n}^t. \quad (51)$$

First, we decode \mathbf{p} and then we find \mathbf{c} . It is interesting to simulate iterative decoding of full-diversity 1-level LDPC lattices for $n = 2$, where the underlying code \mathcal{C} is the $(3, 6)$ ensemble (generalizations to other degree distributions and rates are treated similarly). The Tanner graph of this lattice is presented in Fig. 1. Transmitted information symbols are split into two classes: N symbols are transmitted on h_1 , while N symbols are transmitted on h_2 . Thus, there are two types of edges in Fig. 1. Solid-line edges connect a variable node to a check node, both affected by h_1 , and dashed-line edges connect a variable node to a check node, both affected by h_2 . Due to the structure of the parity check matrix of full-diversity 1-level LDPC lattice in Theorem 7, there is no edge between the affected variable nodes by h_1 and the affected check nodes by h_2 , conversely, there is no edge between the affected variable nodes by h_2 and the affected

check nodes by h_1 . For each variable node ϑ_i , $i = 1, \dots, N$, and check node Φ_j , $j = 1, \dots, k$, we denote by $e_{i,j}$ and $e'_{i,j}$ the edges that connect ϑ_i to Φ_j in the affected part by h_1 and h_2 , respectively. Indeed, $e_{i,j}$ is one of the solid-line edges while $e'_{i,j}$ is one of the dashed-line edges. Only one of these two edges with smaller fading effect, is chosen for decoding. This guarantees full-diversity under iterative message passing decoding [22].

Example 5: Let \mathcal{C} be a binary LDPC code with parity check matrix $\mathbf{H}_{\mathcal{C}}$ as follows

$$\mathbf{H}_{\mathcal{C}} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}. \quad (52)$$

A full diversity 1-level LDPC lattice with diversity order 3 has the following parity check matrix

$$\mathbf{H}_{\Lambda} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (53)$$

The Tanner graph of this lattice is presented in Fig. 2. For decoding, we use the Tanner graph in Fig. 3 in which the solid line edges, corresponding to the edges with lower fading effect, are used in iterative decoding. Indeed, if we apply the Tanner graph of Fig. 2 for our iterative decoding, the generated messages during the message passing iterations will not necessarily preserve full diversity [22]. In Fig. 3, the specified groups of nodes in Fig. 2 inside the dashed-line circles are merged. \square

Define $\hat{\mathbf{p}}$, the estimation of \mathbf{p} , as follows

$$\hat{\mathbf{p}} = Q_{\Lambda'_P}(\mathbf{y}^t), \quad (54)$$

where Λ'_P is the lattice with the following generator matrix \mathbf{P}' and $Q_{\Lambda'_P}(\mathbf{y}^t)$ returns the $\text{argmin}_{\mathbf{z} \in \mathbb{Z}^{nN}} \|\mathbf{y}^t - \mathbf{P}'\mathbf{z}^t\|^2$ with

$$\mathbf{P}' = 2(\mathbf{I}_N \otimes \mathbf{H}_{\mathbf{F}}\mathbf{P}^t),$$

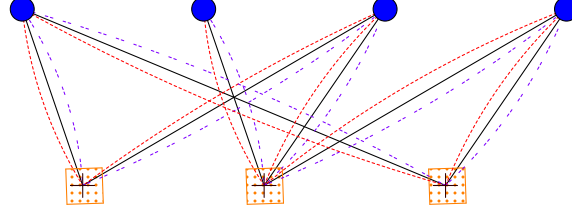


Fig. 3. Tanner graph of a full diversity 1-level LDPC lattice after choosing the edges with the least fading effect.

in which \mathbf{P} is the generator matrix of \mathfrak{P} in \mathbb{R}^n . This decoding step seems to be a hard problem due to the high dimension of Λ'_P which is nN . Here, we present a method which makes the complexity of this step affordable. We use the following property of the Kronecker product in simplifying matrix equations. Consider three matrices \mathbf{A} , \mathbf{B} and \mathbf{X} such that $\mathbf{C} = \mathbf{A}\mathbf{X}\mathbf{B}$. Then [49]

$$(\mathbf{B}^t \otimes \mathbf{A})\text{vec}(\mathbf{X}) = \text{vec}(\mathbf{C}), \quad (55)$$

where $\text{vec}(\mathbf{X})$ denotes the vectorization of the matrix \mathbf{X} formed by stacking the columns of \mathbf{X} into a single column vector. For each $\mathbf{z} = (z_1, \dots, z_{nN}) \in \mathbb{Z}^{nN}$, we consider

$$\mathbf{Z} = \begin{bmatrix} z_1 & z_{n+1} & \cdots & z_{(n-1)N+1} \\ z_2 & z_{n+2} & \cdots & z_{(n-1)N+2} \\ \vdots & \vdots & \ddots & \vdots \\ z_n & z_{2n} & \cdots & z_{nN} \end{bmatrix}.$$

It is clear that $\text{vec}(\mathbf{Z}) = \mathbf{z}^t$. By using (55), we have

$$\begin{aligned} \mathbf{P}'\mathbf{z}^t &= 2(\text{vec}(\mathbf{H}_F\mathbf{P}^t\mathbf{Z})) \\ &= (2\mathbf{z}_1^t\mathbf{P}\mathbf{H}_F, \dots, 2\mathbf{z}_N^t\mathbf{P}\mathbf{H}_F)^t, \end{aligned}$$

where \mathbf{z}_i is the i th column of \mathbf{Z} , for $i = 1, \dots, N$. In a similar manner we can write

$$(\mathbf{I}_N \otimes \mathbf{H}_F)\mathbf{x}^t = (\mathbf{x}_1^t\mathbf{H}_F, \dots, \mathbf{x}_N^t\mathbf{H}_F)^t,$$

where $\mathbf{x}_i^t = \mathbf{x}((i-1)n+1 : in)$, for $i = 1, \dots, N$. Consequently, we have

$$\|\mathbf{y}^t - \mathbf{P}'\mathbf{z}^t\|^2 = \sum_{i=1}^N \|\mathbf{y}_i^t - 2\mathbf{H}_F\mathbf{P}\mathbf{z}_i\|^2,$$

where

$$\begin{aligned}\mathbf{y}'_i &= 2\mathbf{x}_i^t \mathbf{H}_F - (1, \dots, 1) + \mathbf{n}_i \\ &= 2\mathbf{y}((i-1)n+1 : in) - (1, \dots, 1),\end{aligned}$$

and $\mathbf{z}_i^t = \mathbf{z}((i-1)n+1 : in)$. Indeed, it is enough to find $\operatorname{argmin}_{\mathbf{z}_i \in \mathbb{Z}^n} \|\mathbf{y}'_i - 2\mathbf{H}_F \mathbf{P} \mathbf{z}_i\|^2$, for $i = 1, \dots, N$, which are N instances of maximum likelihood (ML) decoding in dimension n . Since n is the number of fading blocks, n is small in comparison to the dimension of lattice $\Lambda = \sigma^N(\Gamma_C)$. For computing the ML solutions, less complex methods exist; one of the most prominent ones being sphere decoding which is based on searching for the closest lattice point within a given hyper-sphere [48]. In small dimensions, typically less than 100, sphere decoding is feasible after computing the Gram matrix [48]. The steps for estimating $\hat{\mathbf{p}}$ is presented in Algorithm 1. The inputs of this algorithm are $\mathbf{P}, \mathbf{H}_F, \mathbf{y}$ and \mathbf{R} , where

$$\mathbf{R} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ -1 & 1 & 0 & \cdots & 0 & 0 \\ -1 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -1 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix},$$

is the $n \times n$ noise reduction matrix that mitigates the effect of the noise created by $\mathbf{c} \otimes (1, \dots, 1)$ in the estimation of \mathbf{p} . We call the matrix $\mathbf{R}^{(1 \leftrightarrow j)}$ in Algorithm 1, for $j = 1, \dots, n$, the $(1 \leftrightarrow j)$ -*row-column permutation* (RCP) of \mathbf{R} , which is obtained by changing the position of the rows j and 1 in \mathbf{R} (denote the obtained matrix by \mathbf{R}') followed by changing the position of the columns j and 1 in \mathbf{R}' . The role of matrix \mathbf{R} and its RCPs are vital because without multiplying by them, the ML decoding in the lattice generated by \mathbf{P} encounters with a noise with variance $\sigma_b'^2 + 4p_i(1-p_i)$, where $p_i = \Pr\{c_i = 1\}$, for $i = 1, \dots, N$ and σ_b' is the variance of the product distribution of h_i and c_i . The lattice generated by \mathbf{P} has small volume and ML decoding can not afford such a big noise. The simulation results show that using our matrix \mathbf{R} significantly improves the performance. The matrix $\mathbf{H}_F^{-1} = (h'_{i,j})$ in Algorithm 1 is an $n \times n$ matrix given as follows

$$h'_{i,j} = \begin{cases} \frac{1}{h_{i,j}}, & \text{if } i = j \text{ and } h_{i,j} \neq 0, \\ 0, & \text{otherwise.} \end{cases} \quad (56)$$

After finding $\hat{\mathbf{p}}$, the estimation of \mathbf{p} , we need to find \mathbf{c} . After choosing the appropriate edges

Algorithm 1 First step of decoding for full diversity 1-level LDPC lattices

```

1: procedure MI-ML( $\mathbf{P}, \mathbf{R}, \mathbf{y}, \mathbf{H}_F = \text{diag}(|h_1|, \dots, |h_n|)$ )
2:    $\hat{\mathbf{y}}, \hat{\mathbf{h}}, \hat{\mathbf{p}} \leftarrow \mathbf{0}_{1 \times N}$ 
3:   for  $i = 1 : N$  do
4:      $\mathbf{y}'_i \leftarrow \mathbf{y}(n(i-1) + 1 : ni)$ 
5:      $i_0 \leftarrow \arg \max_{1 \leq i \leq n} (|h_1|, \dots, |h_n|)$ 
6:      $\mathbf{y}''_i \leftarrow \mathbf{R}^{(1 \leftrightarrow i_0)} \mathbf{H}_F^{-1} \mathbf{y}'_i$ 
7:      $\hat{\mathbf{z}}_i^t \leftarrow \arg \min_{\mathbf{z}_i \in \mathbb{Z}^n} \|\mathbf{y}''_i - 2\mathbf{R}^{(1 \leftrightarrow i_0)} \mathbf{P} \mathbf{z}_i\|^2$ 
8:      $\mathbf{f} = (f_1, \dots, f_n) \leftarrow \mathbf{y}'_i - 2\hat{\mathbf{z}}_i \mathbf{H}_F \mathbf{P}$ 
9:      $i_m \leftarrow \arg \max_{1 \leq i \leq n} (|f_1|, \dots, |f_n|)$ 
10:     $\hat{\mathbf{p}}_i \leftarrow 2\hat{\mathbf{z}}_i \mathbf{P}$ 
11:     $\hat{\mathbf{y}}(i) \leftarrow \mathbf{y}'_i(i_m) - \mathbf{h}(i_m) \hat{\mathbf{p}}_i(i_m)$ 
12:     $\hat{\mathbf{h}}(i) \leftarrow \mathbf{H}_F(i_m, i_m)$ 
13:     $\hat{\mathbf{p}}(i) \leftarrow \hat{\mathbf{p}}_i(i_m)$ 
14:   end for
15:   return  $\hat{\mathbf{y}}, \hat{\mathbf{h}}, \hat{\mathbf{p}}$ .
16: end procedure

```

and discarding the remaining edges, our proposed algorithm is similar to the sum-product algorithm for LDPC codes in message passing structure [50]. The sum-product algorithm iteratively computes an approximation of the MAP (maximum a posteriori probability) value for each code bit. The inputs are the log likelihood ratios (LLR) for the a priori message probabilities from each channel. In the sequel, we introduce our method to estimate the vector of log likelihood ratios $\gamma = (\gamma_1, \dots, \gamma_N)$ for 1-level LDPC lattices in the presence of perfect CSI. We define the vector of log likelihood ratios as $\gamma = (2\hat{\mathbf{h}} \circ \hat{\mathbf{y}})/\sigma^2$, where \circ is the Hadamard product or entrywise product. Then, we input γ to the sum-product decoder of LDPC codes that gives us $\hat{\mathbf{c}}$. We convert $\hat{\mathbf{c}}$ to ± 1 notation and we denote the obtained vector by $\hat{\mathbf{c}}'$. The final decoded lattice vector is

$$\hat{\mathbf{x}} = \hat{\mathbf{c}}' \otimes \overbrace{(1, \dots, 1)}^n + \hat{\mathbf{p}}.$$

Decoding error happens when $\hat{\mathbf{c}} \neq \mathbf{c}$ or $\hat{\mathbf{p}} \neq \mathbf{p}$.

A. Decoding analysis

In this section, we prove that a 1-level LDPC lattice with diversity n achieves diversity $n - 1$ under the decoder proposed in the previous section. We also employ the notations introduced in the previous section. In the first part of our decoding algorithm, we have N instances of optimal decoding, for the lattice generated by \mathbf{P} , over an n -block-fading channel. First, we assume that the transmitted codeword \mathbf{c} in (49) is the all zero codeword. In this case, our decoding problem is N instances of optimal decoding over an n -block-fading channel with an additive noise with variance σ_b^2 . The lattice generated by \mathbf{P} comes from an algebraic number field and it has diversity order n . Thus, at high SNRs, i.e., when $\sigma_b^2 \rightarrow 0$, optimal decoding of this lattice admits diversity order n . Now, we consider the general case that $\mathbf{c} = (c_1, \dots, c_N)$ is not the all zero codeword. In this case, the purpose of the instance i of our optimal decoding, for $i = 1, \dots, N$, is to obtain $\mathbf{p}_i = (\sigma_1(p_i), \dots, \sigma_n(p_i)) = (p_{i,1}, \dots, p_{i,n}) \in \mathbf{P}$ from the received vector of the form

$$\mathbf{y}_i = (h_1(p_{i,1} + c_i) + e_{i,1}, \dots, h_n(p_{i,n} + c_i) + e_{i,n})$$

in which $e_{i,j} \sim \mathcal{N}(0, \sigma_b^2)$, for $j = 1, \dots, n$. We consider $e'_{i,j} = h_j c_i + e_{i,j}$ as the effective noise that is not necessarily small in high SNRs and we reach to an error floor in the performance curve. Without loss of generality, assume $h_1 > 0$ is the maximum of $\{h_1, \dots, h_n\}$. Using Step 6 of Algorithm 1 gives

$$\begin{aligned} \mathbf{y}'_i &= (p_{i,1} + c_i + \frac{e_{i,1}}{h_1}, p_{i,2} + c_i + \frac{e_{i,2}}{h_2}, \dots, p_{i,n} + c_i + \frac{e_{i,n}}{h_n}) \mathbf{R}^t \\ &= (p_{i,1} + c_i + \frac{e_{i,1}}{h_1}, p_{i,2} - p_{i,1} + e''_{i,2}, \dots, p_{i,n} - p_{i,1} + e''_{i,n}), \end{aligned}$$

where $e''_{i,j} = \frac{e_{i,j}}{h_j} - \frac{e_{i,1}}{h_1}$, for $j = 2, \dots, n$, is the Gaussian noise with zero mean and variance $\sigma_e^2 = \left(\frac{h_1^2 h_j^2}{h_1^2 + h_j^2} \right) \sigma_b^2$. If the maximum of $\{h_1, \dots, h_n\}$ occurs at h_j , with $j \neq 1$, we use $\mathbf{R}^{(1 \leftrightarrow j)}$ instead of \mathbf{R} . Now, let us consider $n - 2$ deep fades as $h_3 = h_4 = \dots = h_n = 0$. In this case, we have

$$\mathbf{y}'_i = (p_{i,1} + c_i + \frac{e_{i,1}}{h_1}, p_{i,2} - p_{i,1} + e''_{i,2}, e''_{i,3}, \dots, e''_{i,n})^t, \quad (57)$$

which is equivalent to $n - 2$ deep fades over the lattice vector $(p_{i,1}, p_{i,2} - p_{i,1}, \dots, p_{i,n} - p_{i,1})$ in the generated lattice by $\mathbf{R}\mathbf{P}$. It should be noted that \mathbf{R} and its RCPs are unimodular matrices and consequently, multiplication by these matrices generates equivalent lattices to the generated lattice by \mathbf{P} . Due to the ability of \mathbf{P} in affording $n - 2$ deep fades at high SNRs, under optimal

decoding, we are able to decode $(p_{i,1}, p_{i,2} - p_{i,1}, \dots, p_{i,n} - p_{i,1})$ in the generated lattice by **RP**. After multiplying by \mathbf{R}^{-1} , $\hat{\mathbf{p}}_i = (\hat{p}_{i,1}, \hat{p}_{i,2}, \dots, \hat{p}_{i,n})$ is recovered correctly. After N instances, we obtain $\hat{\mathbf{w}} = \sigma^N(\hat{\mathbf{p}}) = (\hat{\mathbf{p}}_1, \dots, \hat{\mathbf{p}}_N)$ as the estimation of $\sigma^N(\mathbf{p})$ in (49). We also conclude from Equation (57) that using underlying LDPC codes with low maximum Hamming weight, lowers $\Pr\{c_i = 1\}$, for $i = 1, \dots, N$, that gives faster convergence of the error performance curve to its asymptotic slope. During Step 8 and Step 9 of Algorithm 1, the edge with smallest fading effect (or higher fading gain) are chosen among the n equivalent edges that connect ϑ_i to its adjacent check nodes. Indeed, considering the output of Step 8 at instance i , which is a vector of length n with j th component as

$$f_j = \begin{cases} 2h_j (p_{i,j} - \hat{p}_{i,j} + \frac{1}{2}) + e_{i,j}, & \text{if } c_i = 1, \\ 2h_j (p_{i,j} - \hat{p}_{i,j} - \frac{1}{2}) + e_{i,j}, & \text{if } c_i = 0, \end{cases}$$

indicates that choosing f_j 's with higher absolute values increases the reliability in the estimation of log likelihood ratios. During this edge discarding process, the nodes that decline the diversity order are removed and the remaining edges are not affected by deep fades. Hence, in presence of $n - 2$ deep fades, the iterative decoding of \mathbf{c} can be accomplished successfully over the obtained Tanner graph at high SNRs.

In order to discuss the decoding complexity of the proposed algorithm, let us consider the complexity of the used optimal decoder in dimension n as $f(n)$, which is a cubic polynomial for sphere decoder in high SNRs. Since our decoding involves N uses of an optimal decoder in dimension n , the complexity of our decoding method is $O(N \cdot f(n)) + O(N \cdot d \cdot t)$ in which t is the maximum number of iterations in the iterative decoding and d is the average column degree of \mathbf{H}_C . This complexity is dominated by $O(N \cdot d \cdot t)$ as N is much greater than n .

VIII. NUMERICAL RESULTS

In this section, we present numerical results of simulating double diversity and triple diversity 1-level LDPC lattices for block-fading channels. Binary and randomly generated MacKay LDPC codes [51] with parity-check matrices of size 50×100 , 250×500 and (167×334) are used in our simulations. Frame error rate (FER) performance of 1-level LDPC lattices are plotted versus $\rho = 1/\sigma^2$ in Fig. 5. In simulations we have used the construction of Theorem 3 with $m = 10$ and the decoding proposed in the previous section. The results for dimension 200 are provided in presence and absence of multiplying by \mathbf{R} in Algorithm 1. We have compared the obtained results with the proposed Poltyrev outage limit in [23]. This outage limit is related

to the fading distribution and determinant of the lattice which itself is related to m and the rate of its underlying code. The Poltyrev outage limit of full diversity 1-level LDPC lattices with different parameters and diversity orders are plotted in Fig. 4. In Fig. 6 we have presented the FER performance of triple diversity 1-level LDPC lattices, obtained from Example 3 by employing $[100, 50]$ and $[334, 167]$ binary LDPC codes as underlying code. The Poltyrev outage limits with diversity order 2 and 3 are plotted for comparison. Due to the results of Fig. 6, triple diversity 1-level LDPC lattices indicate diversity order 2 under the proposed decoding algorithm in Section VII, that confirms the proven result in Section VII-A.

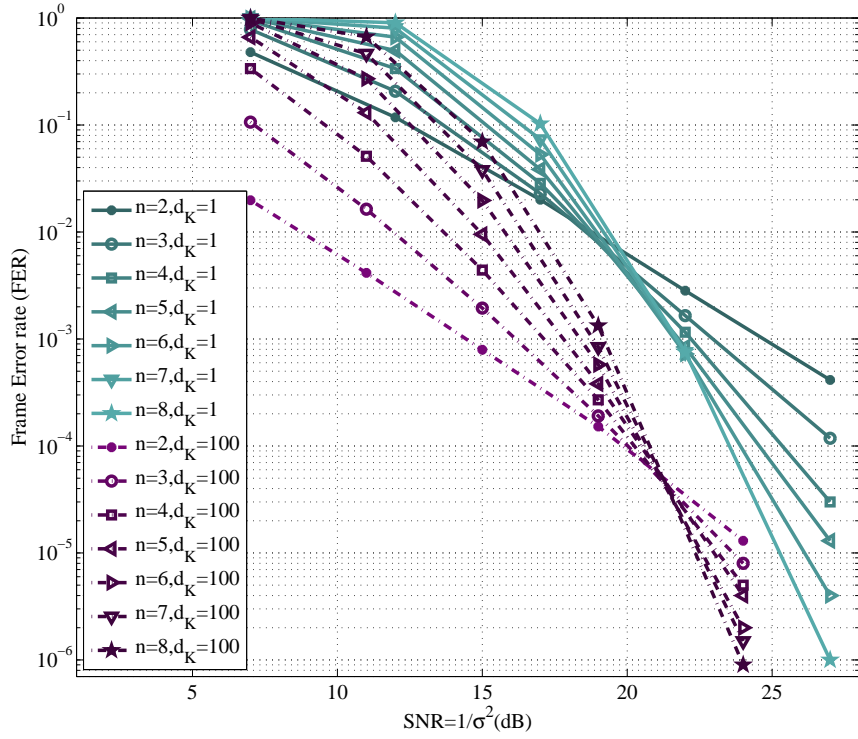


Fig. 4. Poltyrev outage limit for 1-level LDPC lattices with $[N, k] = [100, 50]$ and different diversity orders.

IX. CONCLUSIONS

In this paper, we propose full diversity 1-level LDPC lattices on block-fading channels, based on algebraic number fields. The construction of 1-level LDPC lattices with diversity order 2, 3 and 4 is discussed through the paper. The framework for developing to higher orders of diversity

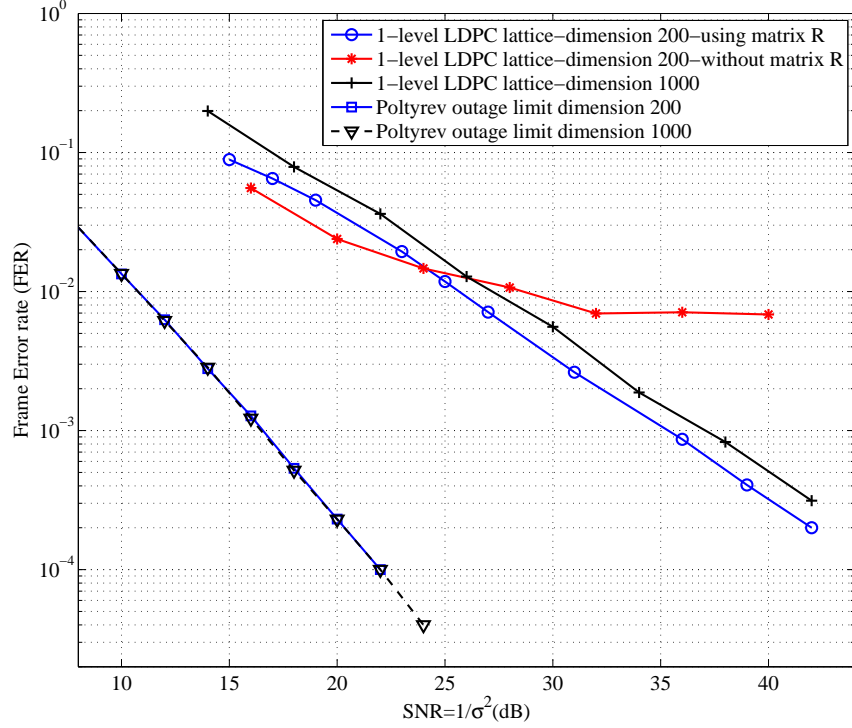


Fig. 5. Decoding of double-diversity 1-level LDPC lattices.

is also provided. In order to apply these structures in practical implementations, we propose a new low complexity decoding method for full diversity 1-level LDPC lattices. The proposed decoder is based on optimal decoding in very small dimensions and iterative decoding. To implement the iterative part of our decoding algorithm, we propose the definition of a parity check matrix and Tanner graph for full diversity Construction A lattices. The proposed decoding algorithm has complexity that grows linearly in the dimension of the lattice that makes it tractable to decode high-dimension 1-level LDPC lattices on the block-fading channel. We also prove that the constructed LDPC lattices together with the proposed decoding method admit diversity order $n - 1$ over an n -block fading channel.

REFERENCES

- [1] H. Khodaiemehr, M.-R. Sadeghi, and D. Panario, "Construction of full-diversity 1-level LDPC lattices for block-fading channels," in *IEEE International Symposium on Inform. Theory (ISIT)*, 2016, Jul. 2016, pp. 2714–2718.
- [2] J. H. Conway and N. J. A. Sloane, *Sphere packing, lattices and groups*. New York: Springer, 1998.
- [3] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Trans. on Inform. Theory*, vol. 40, no. 2, pp. 409–417, Mar. 1994.
- [4] G. D. Forney, M. D. Trott, and S.-Y. Chung, "Sphere-bound-achieving coset codes and multilevel coset codes," *IEEE Trans. on Inform. Theory*, vol. 46, no. 3, pp. 820–850, May 2000.

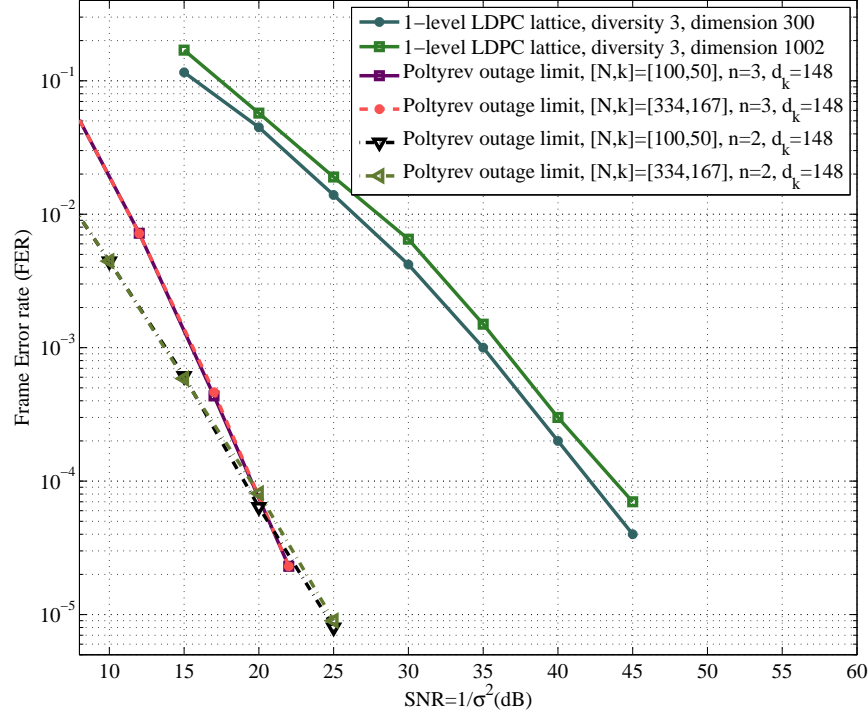


Fig. 6. Decoding of triple-diversity 1-level LDPC lattices.

- [5] U. Erez and R. Zamir, "Achieving $\frac{1}{2} \log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding," *IEEE Trans. on Inform. Theory*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.
- [6] R. Urbanke and B. Rimoldi, "Lattice codes can achieve capacity on the AWGN channel," *IEEE Trans. on Inform. Theory*, vol. 44, no. 1, pp. 273–278, Jan. 1998.
- [7] J. Conway and N. Sloane, "Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice," *IEEE Trans. on Inform. Theory*, vol. 32, no. 1, pp. 41–50, Jan. 1986.
- [8] M.-R. Sadeghi, A. H. Banihashemi, and D. Panario, "Low-density parity-check lattices: Construction and decoding analysis," *IEEE Trans. on Inform. Theory*, vol. 52, no. 10, pp. 4481–4495, Oct. 2006.
- [9] N. di Pietro, J. J. Boutros, G. Zemor, and L. Brunel, "Integer low-density lattices based on construction A," in *IEEE Inform. Theory Workshop (ITW)*, 2012, Sept. 2012, pp. 422–426.
- [10] N. di Pietro, J. J. Boutros, G. Zemor, and L. Brunei, "New results on low-density integer lattices," in *Inform. Theory and Applications Workshop (ITA)*, 2013, Feb. 2013, pp. 1–6.
- [11] N. di Pietro, G. Zemor, and J. J. Boutros, "New results on construction A lattices based on very sparse parity-check matrices," in *IEEE International Symposium on Inform. Theory (ISIT)*, 2013, Jul. 2013, pp. 1675–1679.
- [12] A. Sakzad, M.-R. Sadeghi, and D. Panario, "Construction of turbo lattices," in *48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2010, Sept. 2010, pp. 14–21.
- [13] H. Khodaiemehr, D. Kiani, and M.-R. Sadeghi, "One-level LDPC lattice codes for the relay channels," in *Iran Workshop on Commun. and Inform. Theory (IWCIT)*, 2015, May 2015, pp. 1–6.
- [14] L. Safarnejad and M.-R. Sadeghi, "FFT based sum-product algorithm for decoding LDPC lattices," *IEEE Commun. Letters*, vol. 16, no. 9, pp. 1504–1507, Sept. 2012.

- [15] N. Sommer, M. Feder, and O. Shalvi, "Low-density lattice codes," *IEEE Trans. on Inform. Theory*, vol. 54, no. 4, pp. 1561–1585, Apr. 2008.
- [16] Y. Yan and C. Ling, "A construction of lattices from polar codes," in *IEEE Inform. Theory Workshop (ITW)*, 2012, Sept. 2012, pp. 124–128.
- [17] M.-R. Sadeghi and A. Sakzad, "On the performance of 1-level LDPC lattices," in *Iran Workshop on Commun. and Inform. Theory (IWCIT)*, 2013, May 2013, pp. 1–5.
- [18] W. Ebeling, *Lattices and Codes: A Course Partially Based on Lectures by Friedrich Hirzebruch*, ser. Advanced Lectures in Mathematics. New York: Springer Fachmedien Wiesbaden, 2012.
- [19] W. Kositsattanakarn, S. S. Ong, and F. Oggier, "Construction A of lattices over number fields and block fading (wiretap) coding," *IEEE Trans. on Inform. Theory*, vol. 61, no. 5, pp. 2273–2282, May 2015.
- [20] F. Oggier and E. Viterbo, *Algebraic number theory and code design for Rayleigh fading channels, Foundation and trends in communications and information theory*. Now Publishers Inc, 2004.
- [21] L. H. Ozarow, S. Shamai, and A. D. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Trans. on Vehicular Technology*, vol. 43, no. 2, pp. 359–378, May 1994.
- [22] J. J. Boutros, A. Guillén i Fàbregas, E. Biglieri, and G. Zemor, "Low-density parity-check codes for nonergodic block-fading channels," *IEEE Trans. on Inform. Theory*, vol. 56, no. 9, pp. 4286–4300, Sept. 2010.
- [23] M. Punekar, J. J. Boutros, and E. Biglieri, "A Poltyrev outage limit for lattices," in *IEEE International Symposium on Inform. Theory (ISIT)*, 2015, Jun. 2015, pp. 456–460.
- [24] I. N. Stewart and D. O. Tall, *Algebraic Number Theory*. Chapman and Hall, 1979.
- [25] S. Lang, *Algebraic Number Theory*. Springer-Verlag, 1994.
- [26] P. Samuel, *Théorie Algébrique des Nombres*. Hermann, 1971.
- [27] E. Bayer-Fluckiger, "Lattices and number fields," *Contemp. Math.*, vol. 241, pp. 69–84, 1999.
- [28] D. S. Choie, Y.-J. and H. Liu, "Jacobi forms and Hilbert-Siegel modular forms over totally real fields and self-dual codes over polynomial rings $\mathbb{Z}_m[x]/\langle g(x) \rangle$," *Ars Comb.*, vol. 107, pp. 141–160, Jan. 2012.
- [29] W. Kositsattanakarn, S. S. Ong, and F. Oggier, "Wiretap encoding of lattices from number fields using codes over \mathbb{F}_p ," in *IEEE International Symposium on Inform. Theory Proceedings (ISIT)*, 2013, Jul. 2013, pp. 2612–2616.
- [30] C. Bachoc, "Applications of coding theory to the construction of modular lattices," *Journal of Combinatorial Theory, Series A*, vol. 78, no. 1, pp. 92–119, Apr. 1997.
- [31] S. Dougherty, J.-L. Kim, and Y. Lee, "Codes over rings and Hermitian lattices," *Designs, Codes and Cryptography*, vol. 76, no. 3, pp. 519–535, 2015.
- [32] H. Khodaiemehr, M.-R. Sadeghi, and A. Sakzad, "Practical encoder and decoder for power constrained QC-LDPC lattices," to appear in *IEEE Trans. on Commun.* [Online]. Available: <http://arxiv.org/abs/1603.07010>
- [33] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, ser. Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2004.
- [34] I. Gaal, *Diophantine Equations and Power Integral Bases: New Computational Methods*. Birkhäuser Boston, 2012.
- [35] L. Robertson, "Power bases for cyclotomic integer rings," *Journal of Number Theory*, vol. 69, no. 1, pp. 98 – 118, 1998.
- [36] S. Alaca and K. S. Williams, *Introductory Algebraic Number Theory*. Cambridge University Press, Cambridge, 2004.
- [37] D. Shanks, "The simplest cubic fields," *Mathematics Of Computation*, vol. 28, no. 128, pp. 1137–1152, Oct. 1974.
- [38] J. Proakis, *Digital Communications*, 4th ed. McGraw-Hill, 2001.
- [39] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs and Mathematical Tables*. New York: DoverPress, 1972.
- [40] M. K. Simon and M. S. Alouini, *Digital Communication over Fading Channels*. New York: John Wiley, 2000.

- [41] A. Guillén i Fàbregas and E. Viterbo, "Sphere lower bound for rotated lattice constellations in fading channels," *IEEE Trans. on Wireless Commun.*, vol. 7, no. 3, pp. 825–830, Mar. 2008.
- [42] J. J. Boutros and E. Viterbo, "Signal space diversity: a power- and bandwidth-efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. on Inform. Theory*, vol. 44, no. 4, pp. 1453–1467, Jul. 1998.
- [43] J. J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore, "Good lattice constellations for both Rayleigh fading and Gaussian channels," *IEEE Trans. on Inform. Theory*, vol. 42, no. 2, pp. 502–518, Mar. 1996.
- [44] K. N. Pappi, N. D. Chatzidiamantis, and G. K. Karagiannidis, "Error performance of multidimensional lattice constellations-part II: Evaluation over fading channels," *IEEE Trans. on Commun.*, vol. 61, no. 3, pp. 1099–1110, Mar. 2013.
- [45] C. E. Shannon, "Probability of error for optimal codes in a Gaussian channel," *Bell Syst. Tech. J.*, vol. 38, no. 3, pp. 279–324, May 1959.
- [46] V. Tarokh, A. Vardy, and K. Zeger, "Universal bound on the performance of lattice codes," *IEEE Trans. on Inform. Theory*, vol. 45, no. 2, pp. 670–681, Mar. 1999.
- [47] The Sage Developers, *Sage Mathematics Software (Version 6.9)*, 2015, <http://www.sagemath.org>.
- [48] E. Viterbo and J. J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. on Inform. Theory*, vol. 45, no. 5, pp. 1639–1642, Jul. 1999.
- [49] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*. Cambridge University Press, 1994.
- [50] S. J. Johnson, *Iterative Error Correction*. Cambridge University Press, 2010.
- [51] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. on Inform. Theory*, vol. 45, no. 2, pp. 399–431, Mar. 1999.